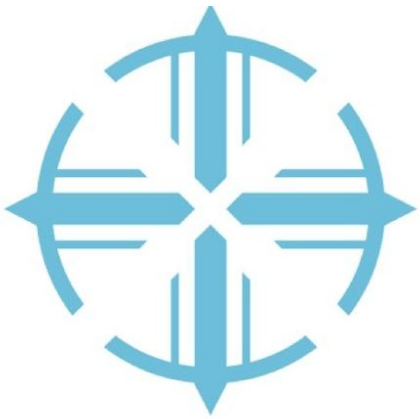
PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS Y COMPUTACIÓN



IMPACTO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (TICS) EN LOS FRAUDES INFORMÁTICOS JUZGADOS EN EL CONSEJO DE LA JUDICATURA DE LA PROVINCIA DE PICHINCHA.

PAULA ROMINA JARAMILLO MONTOYA

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS Y COMPUTACIÓN

Quito, junio 2019

Contenido

Índice de Tablas

Índice de Figuras

Capítulo 1: Definición del Estudio

Introducción

Constantemente se presentan vulnerabilidades en sistemas de información, fallas tanto procedimentales como tecnológicas sobre las infraestructuras de los sistemas implementados de las organizaciones que son infringidas por intrusos informáticos. (López, Amaya, & León, 2004). Es por este motivo que podemos introducirnos en el mundo de la informática forense, que por definición es un proceso metodológico para la recogida y análisis de los datos digitales de un sistema de dispositivos de forma que pueda ser presentado y admitido ante los tribunales.

El presente trabajo de titulación tiene como objetivo analizar las metodologías usadas en los Peritos informáticos del Consejo de la Judicatura en el apoyo al juzgamiento de los delitos presentados en la Provincia de Pichincha y correspondientes al campo de Ingeniería de Sistemas. Para verificar el impacto que tienen las Tecnologías de Información y Comunicación (TICs) en el cometimiento de fraudes y delitos se considera necesario identificar las herramientas y acciones usadas en cada causa (juicio), así mismo, es de importancia conocer el tratamiento que se da a la evidencia digital que durante el proceso pericial. Este trabajo tiene como finalidad visualizar el panorama técnico-legal en el que se encuentra actualmente nuestra sociedad y proponer una metodología para un mejor funcionamiento del sistema.

Antecedentes

Desde la aparición de las Tecnologías de la Información y Comunicación (TICs) en la sociedad se ha modificado la manera de interactuar entre las personas. Consecuentemente, esta evolución no ha dejado de lado al campo penal. Los delincuentes han tomado nuevas formas de infringir la ley. Dentro de los delitos informáticos más comunes encontramos: uso de redes sociales para el acercamiento a menores de edad con fines sexuales, sabotaje informático, conductas dirigidas a daños físicos, conductas dirigidas a daños lógicos. (Camacho, 1987)

En los fraudes informáticos y falsificación electrónica los medios de prueba son de carácter documental y/o material, dado que estas infracciones son de tipo ocupacional. Es decir, El 90% de personas que cometen estos actos delictivos trabajan en la organización que fue víctima; consecuentemente, la prueba de los crímenes se encuentra en los mismos equipos de la organización (Acurio, Delitos Informáticos, 2017).

Industrias tan grandes como la del narcotráfico y el terrorismo están involucradas ya que se utilizan medios tecnológicos para comunicarse y transferir información relevante al propósito. Actualmente, las cifras de crímenes cometidos aumentan exponencialmente en nuestro país.

El enfoque que se quiere dar a esta investigación es presentar una posible solución a esta problemática con herramientas que están disponibles en el mercado y procedimientos de seguridad de la información, que pueden apoyar la actividad de los Peritos y asegurar el uso de la prueba digital en el juzgamiento de los delitos.

Como medida de solución por parte del gobierno el 10 de agosto del 2014 se promulgó en Ecuador el Código Orgánico Integral Penal (COIP) el cual establece sanciones para ciertos delitos informáticos como lo son: la revelación ilegal de base de datos, la interceptación ilegal de datos, la transferencia electrónica de dinero obtenido de forma ilegal, el ataque a la integridad de sistemas informáticos. Sin embargo, cada día existen nuevas modalidades de cometimiento de otros delitos en los que intervienen las TICs.

Situacional general

Alrededor de cuatro mil millones de personas en el mundo tienen acceso a Internet, más del 60% de todos los usuarios de Internet se encuentran en países en desarrollo, y el 45% de todos los usuarios de Internet tienen menos de 25 años. Para el año 2019 se calcula que las suscripciones a banda ancha móvil llegan al 70% de la población total del mundo.

De acuerdo con la información divulgada por la Agencia de Control de las Telecomunicaciones del Ecuador (ARCOTEL) en septiembre de 2018, el Ecuador reportaba una población de 16.961.800 personas y se registran 15.548.544 líneas de telefonía móvil, de estas 8.676.456 poseen acceso móvil a Internet, 10.985.386 están en modalidad prepago y 4.526.908 en pospago.

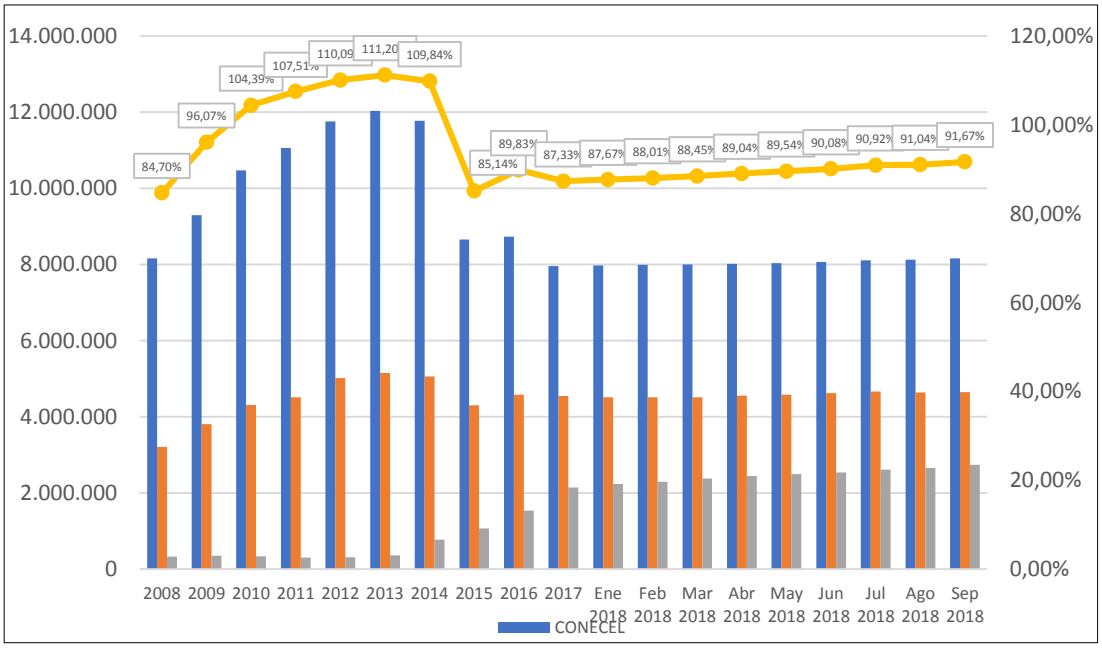


Figura 1: Evolución de Líneas Activas y Densidad
Fuente: Registros administrativos ARCOTEL

Existen 1.913.724 cuentas de Internet fijas en el Ecuador, que corresponden al 11,28% de la población, sin embargo, se estima que a cada cuenta acceden al menos 4 personas; hay 9.059.204 cuentas de Internet que son móviles, es decir el 53,41% de la población lo hacen desde equipos móviles.

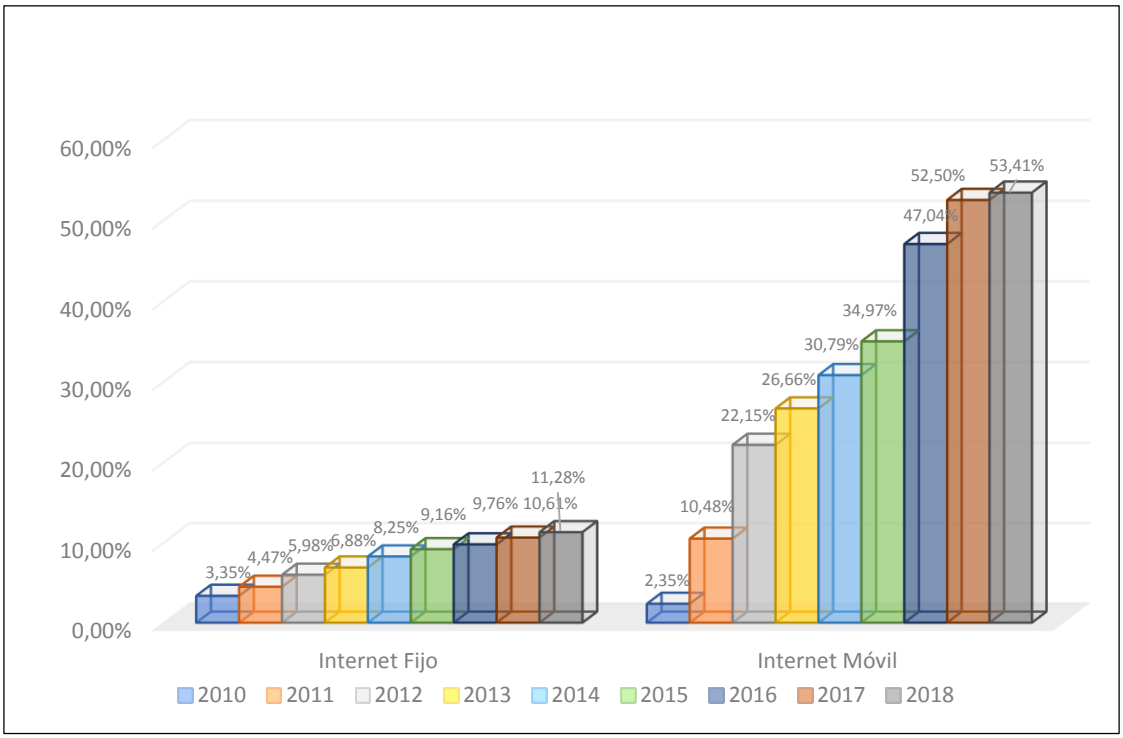


Figura 2: Cuentas Internet Fijo y Móvil por cada 100 habitantes
Fuente: Registros administrativos ARCOTEL

En este mundo hiperconectado, es difícil imaginarse un delito informático otro delito que no involucre evidencia digital vinculada con el uso de TIC´s y la conectividad del Protocolo de Internet (IP).

En el entendimiento de Fabrízio Roza Apud Jesus e Milagre Kohn (Jesus & Milagre, 2018), utiliza el término "Computer Criminals" para designar a los participantes en cometimiento de fraudes, infracciones o delitos por medio de computadores.

Hay otros autores que prefieren la expresión de "crímenes de computador", "cybercrimes", "computer crimes", "delito informático, "crímenes virtuales", "crímenes electrónicos" o incluso "crímenes digitales", "crímenes cibernéticos", "Infocrimenes", "crímenes perpetrados por Internet"; denominaciones distintas, pero que en el fondo significan básicamente la misma cosa. Esto es, un número limitado de actos contra la confidencialidad, la integridad representan el origen del delito informáticos. Pero más allá de eso, los actos informáticos realizados para beneficio, daño personal o financiero, que incluyen formas delincuenciales relacionadas con la identidad y actos

relacionados con contenidos informáticos o uso de Tecnologías de Información y Comunicación (TICs).

El estudio sobre Cibercrimen de la oficina de control de drogas y delitos de la Organización de Naciones Unidas - ONU (ONU, 2013), es una referencia completa para describir cómo el delito cibernético o informático tiene una evolución creciente, a pesar de mostrar estadísticas del año 2013 se consideran de utilidad para describir el problema objeto de este trabajo de titulación, además de que se incluirán datos de años posteriores de otras referencias bibliográficas.

El estudio de la ONU indica que, a nivel mundial, las agencias encargadas de hacer cumplir la ley que respondieron al estudio perciben un aumento en los niveles de delito cibernético, a medida que tanto individuos como grupos delictivos organizados explotan nuevas oportunidades delictivas, impulsados por el lucro y el beneficio personal. Se calcula que más del 80% de los actos de delito cibernético se originan en algún tipo de actividad organizada, con mercados negros de delito cibernético establecidos en un ciclo de creación de programas informáticos maliciosos, infección de computadoras, administración de redes zombi o "Botnet", recolección de datos personales y financieros, venta de datos, y "cobro" a cambio de información financiera.

Los perpetradores de delitos cibernéticos ya no requieren aptitudes o técnicas complejas. En particular en el contexto de los países en desarrollo han surgido subculturas de jóvenes que participan en fraudes financieros informáticos, muchos de los cuales comenzaron a participar en el delito cibernético por lo general a finales de su adolescencia.

A nivel mundial, los actos delictivos cibernéticos muestran una distribución amplia entre actos con motivaciones financieras, actos relacionados con contenidos informáticos y actos contra la confidencialidad, integridad y accesibilidad de los sistemas informáticos. Sin embargo, los gobiernos y las empresas del sector privado perciben la amenaza y el riesgo relativos de manera diferente. Las tasas de delito cibernético registradas por la policía están asociadas con los niveles de desarrollo del país y la capacidad especializada de la policía, y no con las tasas delictivas derivadas de estos delitos. Las encuestas de victimización representan una base más sólida para la comparación. Estas muestran que la victimización individual por delito cibernético es mucho mayor que por las formas de delitos 'convencionales'. Las tasas de victimización por fraude en línea con tarjetas de crédito, robo de identidad, respuesta a intentos de suplantación (phishing) y por experimentar acceso no autorizado a una cuenta de correo varían entre el 1% y el 17% de la población con acceso a Internet, en comparación con tasas de robo, asalto y robo de autos que es de menos del 5%. Las tasas de victimización por delitos cibernéticos son más altas en los países con niveles menores de desarrollo, lo que destaca la necesidad de fortalecer los esfuerzos de prevención en esos países.

Las empresas del sector privado reportan tasas de victimización similares – entre el 2% y el 16% – por actos como el acceso no autorizado a los datos por intrusión o phishing. Las herramientas

delictivas para estos delitos, como las redes zombis “botnets”, tienen un alcance mundial. En 2018 el límite de 4.000 millones de direcciones IP únicas a nivel mundial está por agotarse, y en este universo existen casi 3 millones de direcciones IP que funcionaban como servidores de mando y control de redes zombi (Barrio, 2018). El contenido en Internet también representa una inquietud considerable para los gobiernos. El material al que se dirigen los esfuerzos de remoción no solo incluye la pornografía infantil y el discurso de incitación al odio, sino también contenido relacionado con la difamación y la crítica a personas y gobiernos, lo cual despierta en algunos casos inquietudes relacionadas con las leyes de derechos humanos. Se calcula que casi el 24% de todo el tráfico mundial de Internet viola los derechos de autor, con las descargas de material compartido sin autorización, especialmente en países de África, América del Sur y Asia Occidental y Austral.

La ciberdelincuencia es un área de crimen de rápido crecimiento. Cada vez más delincuentes explotan la velocidad, la comodidad y el anonimato de Internet para cometer distintas actividades delictivas que no conocen fronteras, ya sean físicas o virtuales, causan graves daños y representan amenazas reales para las víctimas en todo el mundo (INTERPOL, 2018).

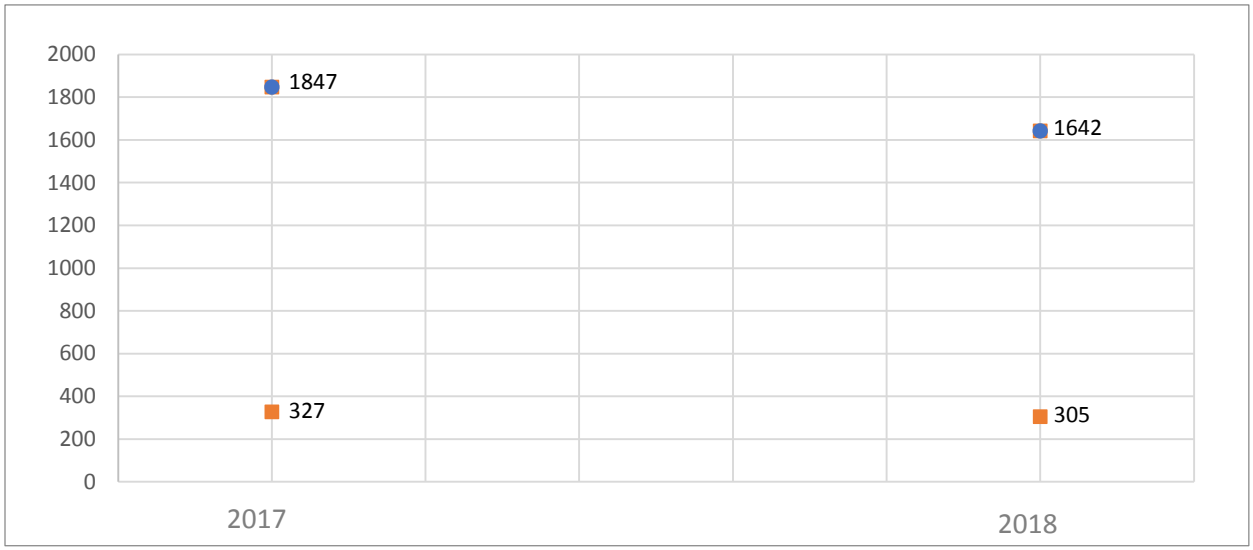


Figura 3: Denuncias por delitos informáticos con intervención de las TICs convertidas en juicios en Ecuador vs. número de delitos con influencia de TICs en Pichincha.
Fuente: Consejo de la Judicatura del Ecuador

Según datos del a la Fiscalía General del Estado las noticias de delitos informáticos se han multiplicado, de 185 denuncias o noticias de delitos en el año 2015 por acceso no consentido a un sistema informático o de telecomunicaciones en el año 2018 se alcanzó a 241, representa un 30% de crecimiento, La apropiación fraudulenta por medios electrónicos registro 958 denuncias en el

año 2017 y subió a 1430 denuncias en el año 2018 mostrando un incremento de casi el 50%; lo que confirma el gran aumento de delitos informáticos y con uso de TICs.

De acuerdo con datos de la Dirección Nacional de Estudios Jurídicos y Estadísticos del Consejo de la Judicatura al 2018, los delitos de Pornografía infantil, violación a la intimidad, estafa, robos, apropiación fraudulenta de medios electrónicos, ataque a sistemas informáticos, entre otros; se han visto influenciados directamente por el uso de TICs e Internet, alcanzando índices como los que se presenta en la figura 4.

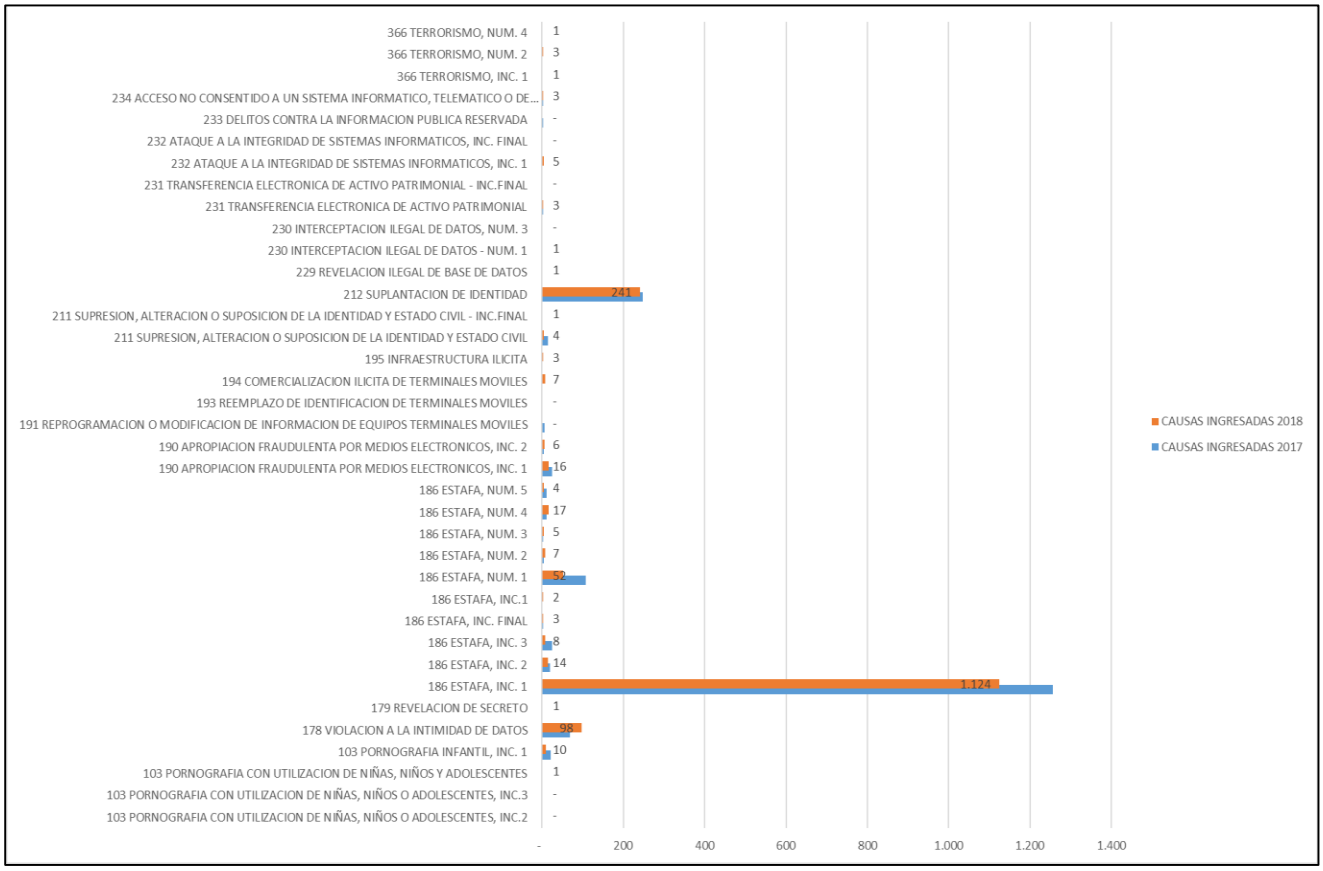


Figura 4: Juicios por delitos con TICS en el Ecuador
Fuente: Dirección Nacional de Estudios Jurídicos y Estadísticos del Consejo de la Judicatura

Actualmente, las estadísticas delictivas registradas por la Fiscalía y Función Judicial no se han evaluado como una base sólida para proponer políticas a nivel nacional, como la adhesión del Ecuador al convenio de Budapest sobre Ciberseguridad.

Objetivos

Objetivo general

- Analizar y verificar el impacto de las Tecnologías de Información y Comunicación (TICS) en los Fraudes Informáticos y juzgamiento correspondiente por parte del Consejo de la Judicatura de la Provincia de Pichincha.

Objetivos específicos

- Recabar toda la información necesaria sobre las actividades y procesos que se han venido llevando a cabo en la investigación y juzgamiento del fraude informático o a través del uso de TICs realizado por el Consejo de la Judicatura
- Describir el funcionamiento de las principales herramientas utilizadas para cometer los delitos de robo, apropiación ilícita y destrucción de sistema informático o red electrónica y otros delitos; al igual que las herramientas para neutralizar estos ataques.
- Analizar las tendencias de los delitos mediante el uso de TICs
- Determinar la importancia de la evidencia digital en la investigación de los delitos.
- Proponer una metodología para apoyar el juzgamiento del uso de TICs en el cometimiento de los delitos de robo, apropiación ilícita y destrucción de sistema informático o red electrónica, y otros, mediante el análisis de los factores que han influido en los casos a estudiar.

Justificación

En el 2017, La Dirección de Política Criminal de la Fiscalía General reporta 6966 noticias de delitos relacionados al uso de TICs, en el año 2018 estas se incrementaron a 8445 y en enero de 2019 ya eran 888, de las denuncias en 2018 327 fueron a juicios y 244 recibieron sentencias y en el año 2017 en tanto se plantearon 305 juicios y 267 fueron sentenciados, lo que demuestra que hoy en día la sociedad ecuatoriana no es la excepción en el auge y crecimiento de delitos cibernéticos; siendo cada vez más afectada por los abusos que se hace de las Tecnologías de Información y Comunicación para actos impropios.

Tabla 1: Delitos Registrados en el periodo 2017-2019

NOTICIAS DE DELITOS	AÑO 2017	AÑO 2018	ENERO 2019
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	220	241	19
Apropiación fraudulenta por medios electrónicos	958	1430	168
Ataque a la integridad de sistemas informáticos	86	88	6
Comercialización ilícita de terminales móviles	24	13	
Delitos contra la información pública reservada legalmente	14	12	
Espionaje	1	1	

Interceptación ilegal de datos	63	41	5
Pornografía con utilización de niñas, niños o adolescentes	107	105	11
Reemplazo de identificación de terminales móviles	5	2	
Reprogramación o modificación de información de equipos terminales móviles	7	4	1
Revelación de secreto (Por parte de profesional que debe guardar reserva)	13	13	2
Revelación ilegal de base de datos	21	45	2
Suplantación de identidad	3672	4177	450
Supresión, alteración o suposición de la identidad y estado civil	52	81	11
Terrorismo	13	90	6
Transferencia Electrónica de activo patrimonial	59	37	3
Violación a la intimidad	1651	2065	204
TOTAL	6966	8445	888

Fuente: Fiscalía General del Estado

A nivel social solo preguntando a amigos y familiares se puede claramente observar cómo con el pasar del tiempo este tipo de delitos ha ido aumentando exponencialmente. Es por esta razón, que se considera necesario investigar las razones y consecuencias que este tipo de actos involucran y cómo influye la prueba pericial técnica en el juzgamiento de estos. Además, se va a estudiar las acciones, métodos y herramientas que han sido utilizadas en algunos los casos seleccionados.

Con esta investigación se plantea proponer una metodología para la investigación forense que permita ayudar a identificar o determinar los autores de los delitos y reducir el número de futuras víctimas a través del uso de medios telemáticos. Como resultado se espera describir los procedimientos que apoyen en las pericias técnicas que hacen los Peritos en informática forense y que se consideran pruebas durante el proceso de juzgamiento.

Alcance

Después de este capítulo introductorio se hará un posicionamiento del problema a través del análisis de las TICs, el uso de Internet y redes sociales, la accesibilidad de telefonía celular móvil a nivel global y nacional.

Se hará un estudio general de los denominados delitos cibernéticos, entendiendo que dentro de estos se encuentran los delitos informáticos y los otros delitos comunes en que se usan TICs para su cometimiento, para la tipificación de este tipo de delitos se buscará una relación de los delitos informáticos con otros delitos tipificados en el Código Integral Penal del Ecuador (COIP). Se pretende hacer un estudio explicativo de la informática forense y su realidad en el Ecuador a través de visitas de campo a las instituciones de la Función Judicial tales como Policía Judicial, Fiscalía y

Juzgados, con el fin de conocer los recursos con que se hace la investigación de los delitos informáticos en nuestro país y contrastar con los estándares que ha impuesto la industria forense. Se comenzará realizando un análisis de las investigaciones realizadas por los Peritos acreditados en informática forense del Consejo de la Judicatura (CJ), para ello con el auspicio del Consejo de la Judicatura se tendrá acceso a una muestra de informes periciales reales presentados en diversas causas en que la prueba digital ha sido de utilidad para su juzgamiento. Del análisis a los informes periciales se pretende determinar la importancia de la prueba digital, hacer una investigación de las herramientas tecnológicas y procedimientos se disponga sobre la investigación de delitos a través del uso de TICs, determinar la incidencia del uso de las TICs en el cometimiento de otros delitos y fraudes informáticos tipificados en el Código Integral Penal del Ecuador.

Para cumplir el análisis propuesto se verificarán las normativas y regulaciones existentes para la prevención, el control e investigación de la incidencia del uso de TICs en el cometimiento de delitos de los casos investigados.

Para finalizar, se propondrá una metodología para investigar los delitos informáticos y otros delitos más frecuentes en que intervienen las TICs de acuerdo con los registros en el Consejo de la Judicatura de Pichincha, dando pautas y proponiendo procedimientos forenses para la utilización de herramientas tecnológicas en la investigación.

Limitaciones

Existen ciertos factores que pueden impedir o dificultar la posibilidad de presentar una certeza total sobre los resultados obtenidos, entre los cuales tenemos:

- Que las autoridades de las instituciones gubernamentales no entreguen la información necesaria oportunamente, completa y como se requiere.
- Que la mayor parte de la información obtenida es de fuentes bibliográficas y documentación de divulgación general sea insuficiente y en caso de requerir información específica no esté disponible o no exista.
- Que los documentos e informes a analizar no estén en concordancia con el tipo de delitos que se asocian al uso de TICs. Sin embargo, la muestra que se tomará es real y se espera que permita identificar los procedimientos y buenas o malas prácticas usadas por los Peritos informáticos; y, a partir de estos proponer una metodología para atenuar las limitaciones que actualmente se presentan tanto en el uso de herramientas tecnológicas como en protocolos y procedimientos autorizados para validar el informe pericial como prueba.

CAPÍTULO 2: Relevamiento de Documentación y Bibliografía

Análisis de bibliografía

La fuente de información principal para este trabajo de titulación es el Consejo de la Judicatura y La Fiscalía General del Estado, por ser las instituciones que disponen de la información referente a lo que se pretende estudiar. Además, se utilizarán los estudios y publicaciones de organismos internacionales y nacionales responsables por la seguridad informática y el control de este tipo de delitos. Otras fuentes serán la Industria y los trabajos de investigación académicos realizados sobre el tema o similares.

En lo referente al juzgamiento de los delitos tenemos como fuente de información el Código Orgánico Integral Penal, este es un conjunto de normas jurídicas donde se establecen los delitos y las penas conforme funciona el sistema judicial ecuatoriano. Existe una serie de artículos que posteriormente se especificará, donde se establece la punición para los infractores de delitos informáticos.

Jhony Enríquez y Yasser Alvarado (Jhony Enriquez, 2015) presentan en su artículo un análisis de los peligros que trajo el crecimiento tecnológico para el uso de delincuentes, clasifican los tipos de delitos informáticos existentes, para luego hacer un análisis de los cometidos en el Ecuador durante el periodo 2010-2015; presentan un análisis de los artículos correspondiente a la sección tercera del COIP que sanciona los delitos informáticos y proponen procedimientos para evitar ser víctimas de estas conductas antisociales.

Juan David Rodríguez (Rodriguez, 2012) en su artículo "Análisis de los Delitos informáticos Presentes en las Redes Sociales en Colombia para el año 2011 y su Regulación", muestra cómo los desarrollos de Tecnologías de Información y Comunicación (TICs) en especial las redes sociales han generado cambios y repercusiones en el comportamiento humano, produciendo transformaciones de los ámbitos jurídicos y sociales; describe los comportamientos que se pueden reconocer como delitos informáticos en dichas redes y cómo se debería adecuar la normativa jurídica en Colombia, para prevenir, proteger y establecer un adecuado manejo de las TICs.

La Facultad de Ciencias Físico Matemáticas de la Universidad Autónoma de Nuevo León, México (Jésus Loredo, 2013) hace conocer los principales delitos informáticos y los riesgos que estos generan en la sociedad, las empresas y los gobiernos; muestra las principales leyes que existen en México para tipificar este tipo de delitos en base a los acuerdos internacionales que ha suscrito México con el fin de combatir este problema.

El centro de educación continua de la Universidad Técnica Particular de Loja, dicta seminarios sobre control de delitos informáticos para el Ecuador dirigido a profesionales de carreras afines a las ciencias jurídicas en respuesta a la creciente necesidad de entender cómo los ataques a personas e infraestructuras tecnológicas se podrían enlazar con los artículos del COIP de la

Republica del Ecuador; en estas actividades se logra asociar los artículos del COIP con otros delitos comunes tales como pornografía, pornografía infantil, fallos, vulnerabilidades y accesos no autorizados a sistemas, estafas, secuestro, robo de identidad, robo de información, utilización no autorizada de servicios principalmente.

Danic Maldonado (Maldonado, 2015) miembro de la policía de investigaciones de Chile en su conferencia sobre delitos informáticos y la ciberseguridad desde un enfoque policial presenta la identificación de delitos cibernéticos y su clasificación en delitos informáticos y computacionales. Muestra cómo el gran número de aplicaciones informáticas presentes en Internet pueden influir en la sociedad y en el cometimiento de delitos. Describe el aparecimiento de nuevas "Naciones Digitales" tales como Facebook, YouTube, WhatsApp que poseen miles de millones de usuarios, y son más grandes que la población de muchos países del mundo. Así mismo, cómo estas redes son utilizadas en el cometimiento de delitos informáticos y otros tradicionales (pornografía infantil, abuso sexual impropio, propiedad intelectual, estafa, usurpación de nombre). Describe los procedimientos que usan los delincuentes y hace una reflexión sobre la conciencia de seguridad que deben tener los usuarios de redes sociales.

El Dr. Santiago Acurio del Pino en su artículo "Delitos Informáticos: Generalidades" (Acurio, Delitos Informáticos, 2017) hace una delimitación del fenómeno de la delincuencia informática definiendo y conceptualizando los delitos informáticos, presenta como tipos de delitos informáticos: los fraudes, el sabotaje informático, el espionaje informático, el hurto de software, el robo de servicios y el acceso no autorizado a servicios informáticos. Hace un análisis de cómo se ha tratado este problema en otros países en organismos como las Naciones Unidas, la Organización de Estados Americanos y la Unión Europea. Describe el problema de la persecución y judicialización de este tipo de delitos ante la realidad procesal del Ecuador.

Luis Jara Obregón y Enrique Ferruzola en su trabajo "Delitos a través de Redes Sociales en el Ecuador" (Jara & Ferruzola, 2017) muestran la conceptualización de los principales delitos que se cometen comúnmente usando redes sociales; presentan los métodos y técnicas que usan los denominados ciberdelincuentes en Internet para acercarse a sus víctimas y crear el ambiente para el cometimiento del delito. Investigan el marco jurídico para hacer frente a estas prácticas dentro del COIP en el Ecuador. Hacen un estudio de campo a través de entrevistas y encuestas a fiscales y elementos de la Policía Judicial de la provincia del Azuay tendientes a determinar cuáles son los procesos que se siguen en la investigación de este tipo de delitos.

Andrés Llangarí en su trabajo de titulación "Análisis de los Delitos Informáticos y de Telecomunicaciones en el Ecuador" (Llangari, 2016) hace un análisis de los delitos informáticos y de telecomunicaciones en base a los cuerpos jurídicos existentes en el Ecuador, tendiendo a hacer una correcta interpretación y comparación del delito y su tipificación, describe los medios tecnológicos que se ocupan para realizar estos actos ilícitos y muestra los procedimientos que el

Ecuador pretende ejecutar para garantizar la seguridad de la información en las instituciones públicas y privadas.

La Fiscalía General del Estado ha elaborado el manual para el manejo de evidencias digitales; la Policía Judicial del Ecuador ha implementado un laboratorio forense con herramientas tecnológicas para la investigación de los delitos en donde intervienen Tecnologías de Información tales como Encase, UFED- Cellebrite, Autopsy, FTK, entre otras.

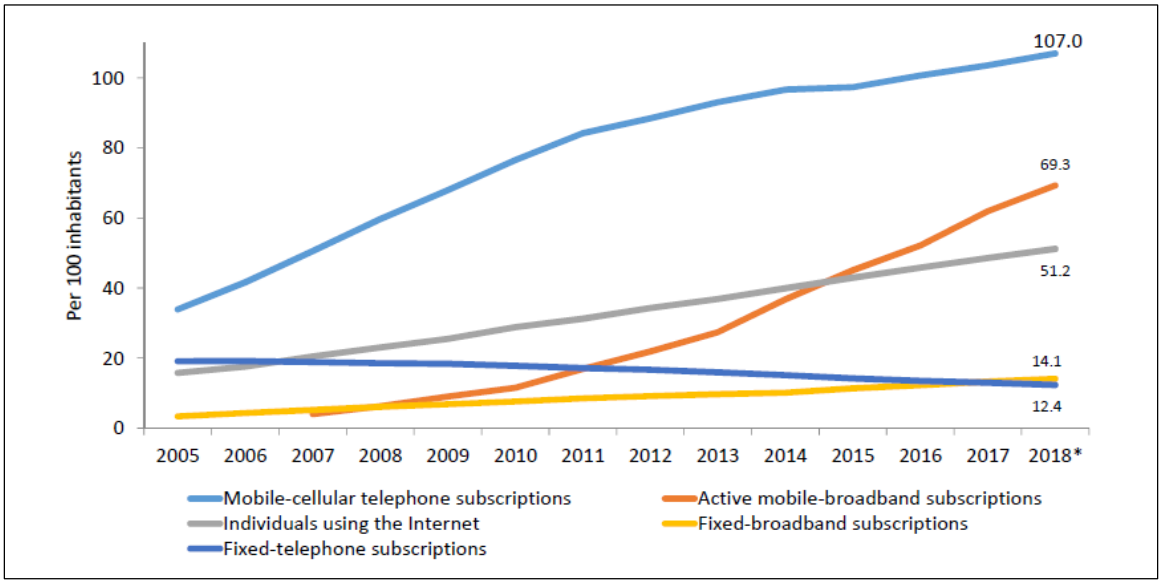


Figura 5: Situación de las TICS - Desarrollo de las TICs 2005-2018
Fuente: ITU Unión Internacional de Telecomunicaciones – UIT

Con base en el informe sobre la Medición de la Sociedad de la Información 2018 de Unión Internacional de Telecomunicaciones - UIT (International Telecommunication Union, 2018) en el año 2018, el 51,2% de la población mundial, es decir, 3 900 millones de personas utilizan Internet. El estudio se ha analizado en base a los reportes de tres tipos de países: los denominados desarrollados, los en desarrollo y los menos desarrollados. Así, en los países desarrollados, cuatro de cada cinco personas están en línea, alcanzando niveles de saturación. En los países en desarrollo, como el Ecuador, todavía hay un amplio margen para el crecimiento, ya que sólo el 45% de las personas utilizan Internet. En los 47 países menos adelantados (PMA, en ingles LDC) del mundo, la utilización de Internet sigue siendo relativamente escasa, a saber, cuatro de cada cinco personas (80%) aún no están conectadas.

Mientras que el número de usuarios (abonados) de la telefonía fija está disminuyendo, los abonados de la telefonía móvil celular ya son mayor que la población mundial.

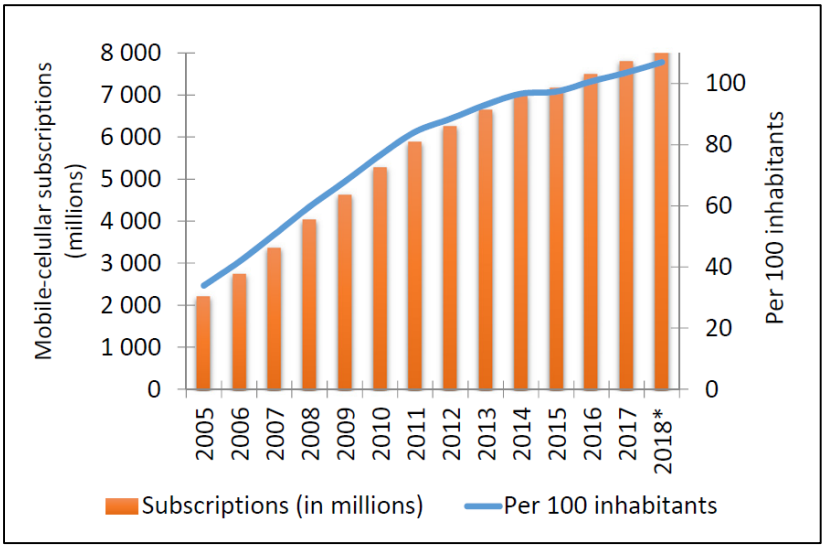


Figura 6: Número de suscriptores de telefonía móvil celular total y por cada 100 habitantes 2005-2018
Fuente: International Telecommunication Union

El acceso a la banda ancha también está en crecimiento, el número de abonados de banda ancha fija (en hogares y oficinas) aumentan constantemente, estos abonados tienen una velocidad de descarga mínima de 2Mbit/s, y una parte considerable posee velocidades mayores a 10 Mbit/s. se estima que 70 de cada 100 habitantes ya poseen acceso banda ancha móvil.

Casi toda la población mundial tiene alcance a la telefonía móvil celular, teniendo acceso a Internet móvil a través de redes 3G o de mayor calidad. Se determina incluso que la penetración y evolución de la red móvil es más rápida que el crecimiento en el porcentaje de la población que utiliza Internet.

En el 2018 el 60% de los hogares cuentan con acceso a Internet. El 45% de la población mundial posee un equipo computacional, en los países en desarrollo el 30% de los hogares tienen acceso a un computador y en los países desarrollados el 75 % de los hogares.

El 92% de las personas en países desarrollados son propietarios de un teléfono celular y 70 de cada 100 personas en países en desarrollo poseen un celular.

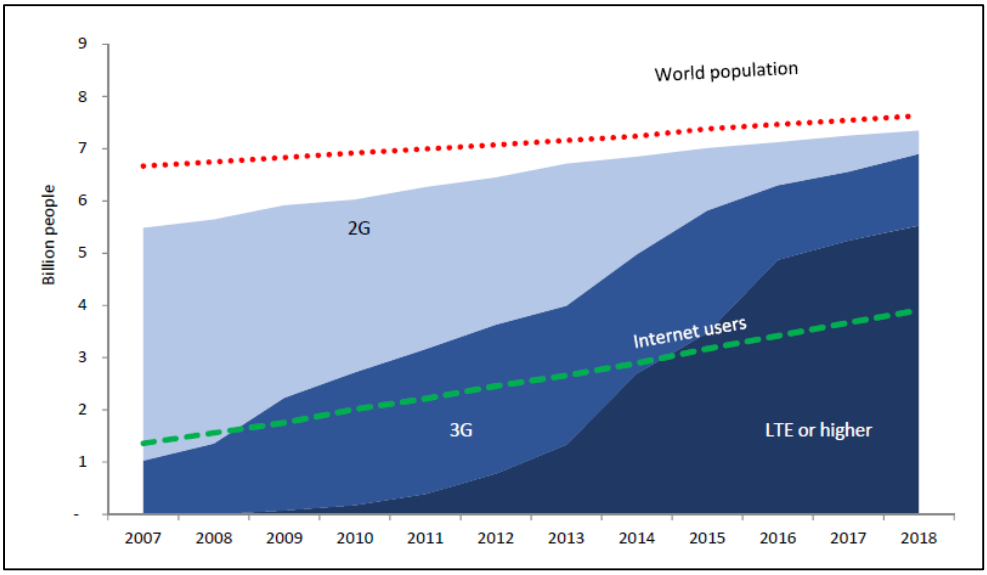


Figura 7: Cobertura móvil por tipo de red 2007-2018
Fuente: International Telecommunication Union

El crecimiento del ancho de banda internacional y del tráfico de Internet ha sido mayor que el crecimiento del acceso a las TICs y mayor que la población que utiliza Internet, lo que se explica por el hecho de que las personas en línea pasan más tiempo en actividades con gran flujo de datos, como ver videos o juegos interactivos.

Con referencia a las aptitudes de las TICs, el informe de la UIT muestra que existe deficiencias en todos los niveles en cuanto a las aptitudes necesarias para el uso de TICs, así, una tercera parte de las personas carece de conocimientos básicos de informática, tales como copiar archivos o carpetas, solamente el 41% tiene conocimientos básicos, tales como instalar o configurar programas informáticos o utilizar fórmulas básicas de hojas de cálculo; y solamente el 4% usa un lenguaje especializado para escribir programas informáticos.

La falta de datos indica que los países en desarrollo se encuentran en desventaja en lo referente a competencias digitales sean estas básicas o generales. Incluso dentro de un mismo país las desigualdades entre competencias básicas y generales corresponden a patrones históricos de desigualdad, en promedio las personas con empleo tienen 10% más de probabilidad de estar calificados que los trabajadores autónomos. Y estos a su vez un 10% más que los desempleados.

Las personas con educación de tercer nivel tienen 1,5 a 2 veces más probabilidad de adquirir aptitudes que las de formación secundaria y de 3,5 a 4 veces más probabilidad de las que solo tienen primaria.

La desigualdad de aptitudes digitales es similar entre niños que entre adultos por lo que no se considera algo generacional ni que persista en el futuro. Se determina que la máxima prioridad

debe ser mejorar la eficiencia de las políticas en materia de aptitudes digitales en relación con las carencias en el mercado laboral y la preocupante ampliación de las desigualdades sociales.

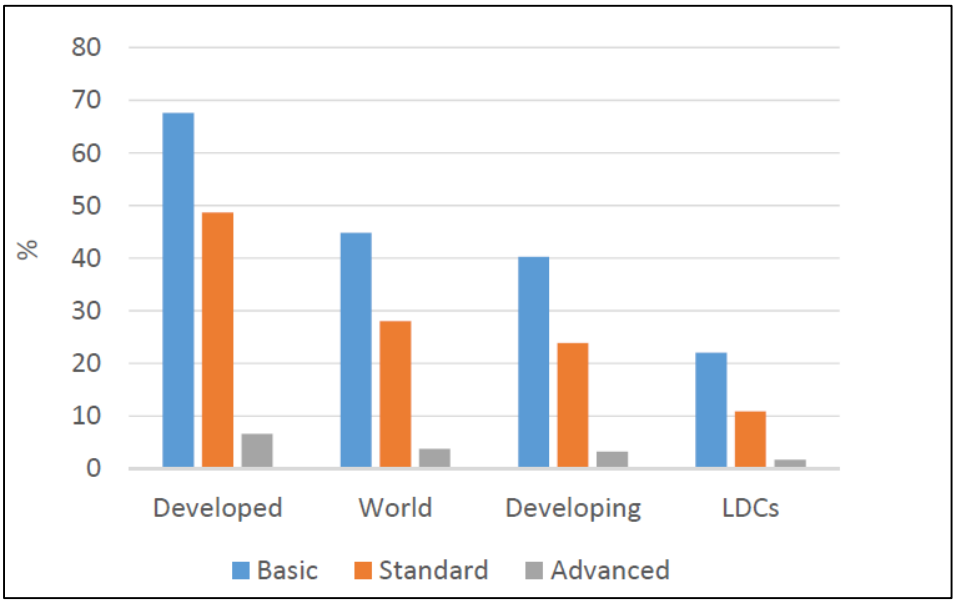


Figura 8: Porcentaje de personas con habilidades y competencias en el uso de TICs por nivel de desarrollo -2017
Fuente: International Telecommunication Union

Es en este entorno del mundo digital en el que se mueven las personas para usar las TICs en sus actividades cotidianas y es en este mismo entorno en el que los delincuentes han encontrado una oportunidad para delinquir y no ser identificado, peor aún juzgado.

Uso de Internet y Redes Sociales

Para desarrollar este acápite se ha seleccionado como fuente el estudio Simon Kemmp (Kemp, 2019) Informe de 2019 de Hootsuite y "We Are Social", en el que permite revelar la realidad del uso de Internet y redes sociales en el mundo para posteriormente presentar la realidad del Ecuador que es de interés del presente trabajo de titulación.

Se muestra que la cantidad de personas que utilizan Internet ha aumentado con más de un millón de personas conectándose por primera vez cada día desde enero de 2018. no son solo los usuarios de Internet los que han estado creciendo, sino también una nueva y extensa oferta de servicios digitales.

Así, indica que de los 7.676 millones de personas que hay en el mundo, el 56% están en ciudades y sitios urbanos, es decir 4.299 millones de personas; para esta población se prestan los siguientes servicios tecnológicos:

Tabla 2: Usuarios de servicios tecnológicos

No. (Millones)	Servicio digital
5.112	Usuarios de telefonía móvil
4.388	Usuarios de Internet
3.484	Cuantas activas en redes sociales
3.256	Usuarios de redes sociales en equipos móviles

Fuente: Informe de 2019 de Hootsuite

Tabla 3: Hallazgos del informe "Digital in 2019"

2018		2019			Crecimiento (%)
5.01	Mil Millones	5.11	Mil Millones	Usuarios móviles únicos en el mundo	2%
3.99	Billones	4.39	Billones	Usuarios de Internet	9%
3.166	Mil Millones	3.48	Mil Millones	Usuarios en redes sociales	9%
2.934	Mil Millones	3.26	Mil millones	Usuarios que utilizan redes sociales en dispositivos móviles	10%

Fuente: Informe de 2019 de Hootsuite

Tabla 4: Penetración de Internet

73%	Sur América
95%	Estados Unidos y Europa
42%	En países menos desarrollados

Fuente: Informe de 2019 de Hootsuite

Comportamientos de los usuarios de Internet en 2019

Las formas en que las personas usan Internet también están evolucionando rápidamente, con el acceso a redes móviles para una parte cada vez mayor de nuestras actividades en línea. A seguir se presenta los aspectos específicos del uso de aplicaciones y dispositivos móviles, ya que los teléfonos móviles representan casi la mitad del tiempo que las personas pasan en Internet.

Google es el sitio web más visitado del mundo, según datos de las empresas especializadas en medición SimilarWeb y Alexa. La otra gran plataforma de Alphabet, YouTube, ocupa el segundo lugar en ambas listas, mientras que Facebook ocupa el tercer lugar.

Tabla 5: Sitios Web más visitados

Ord.	Sitio Web	Categoría	Tiempo de visita
1	Google.com	búsqueda	09m12s
2	YouTube.com	Video	21m36s

3	Facebook.com	Social	11m44s
4	Baidu.com	Búsqueda	06m53s
5	Wikipedia.org	Referencia	03m45s
6	Yahoo.com	Portal	06m26s
7	Twitter.com	Social	09m14s
8	Pornhub.com	Adultos	10m16s
9	Yandex.ru	Búsqueda	10m43s
10	Instagram.com	Social	06m25s
11	Amazon.com	Compras	06m18s
12	Xvideos.com	Adultos	12m34s
13	Xnxx.com	Adultos	14m39s
14	Amproject.org	Noticias	03m53s
15	Live.com	Correo	07m15s
16	Vk.com	Social	16m50s
17	Netflix.com	Video	09m14s
18	Qq.com	Portal	04m00s
19	Mail.ru	Portal	07m38ss
20	Reddit.com	Social	09m13s

Fuente: Ranking de Similar Web basados en el tráfico global

Se evidencia que las plataformas de medios sociales tienen una gran presencia en las listas de los sitios más visitados. Los sitios de comercio electrónico han aumentado constantemente entre los sitios más visitados, los últimos datos de Alexa colocan a 5 sitios de comercio electrónico entre los 20 primeros puestos.

Tabla 6: Sitios web más visitados en el mundo

Ord.	Sitio Web	Tiempo de visita por día	Paginas por visitas
1	Google.com	07m42s	9.54
2	You Tube.com	08m47s	5.02
3	Facebook.com	09m43s	4.03

4	Baidu.com	07m21s	5.60
5	Wikipedia.org	04m15s	3.16
6	Qq.com	04m00s	3.81
7	Taobao.com	07m55s	4.07
8	Tmail.com	07m27s	2.92
9	Amazon.com	04m01s	9.26
10	Yahoo.com	04m01s	3.60
11	Twitter.com	06m23s	3.21
12	Sohu.com	04m03s	4.09
13	Jo.com	04m57s	5.44
14	Live.com	03m53s	3.76
15	Reddit.com	11m40s	7.54
16	Vk.com	10m04s	4.69
17	Instagram.com	05m47s	3.86
18	Weibo.com	05m35s	4.31
19	Sina.com.cn	03m09s	3.20
20	Yandex.ru	06m35s	3.38

Fuente: Ranking Alexa basado en el número de visitantes y total de páginas vistas

Los sitios "para adultos" aparecen con fuerza en los rankings de SimilarWeb también, aunque los datos de Alexa cuentan una historia ligeramente diferente. La tabla de Alexa refleja que las personas pasan mucho tiempo consumiendo contenido para adultos.

Usuarios de redes sociales en 2019

El número de usuarios de redes sociales en todo el mundo ha aumentado a casi 3,5 mil millones a principios de 2019, con 288 millones de usuarios nuevos en los últimos 12 meses, lo que ha llevado la cifra de penetración global al 45% y en Sur América la penetración es del 66% basado en la actividad de los usuarios en plataformas sociales encada país comparado con la población del país.

Comportamientos de las redes sociales en 2019

GlobalWebIndex informa que el usuario promedio de las redes sociales ahora pasa 2 horas y 16 minutos cada día en plataformas sociales, lo que equivale a aproximadamente un tercio de su tiempo total de Internet y una séptima parte de su tiempo.

El tiempo empleado en las redes sociales varía considerablemente según las culturas, aunque los usuarios de Internet en Japón gastan un promedio de solo 36 minutos en las redes sociales cada día. En el otro extremo de la escala, los filipinos que pasan la mayor parte del tiempo en las redes sociales, con un promedio de 4 horas y 12 minutos.

Principales plataformas de redes sociales en 2019

Facebook mantiene su clasificación de plataforma superior, de hecho, los números mensuales de usuarios activos (MAU) de Facebook aumentaron; la compañía anunció que había superado los 1.000 millones de "cuentas activas".

Usuarios móviles en 2019

La cantidad de personas en todo el mundo que usan un teléfono móvil son más de 5,1 mil millones de usuarios en enero de 2019. Esta cifra eleva la penetración de dispositivos móviles en todo el mundo al 60 % es decir alcanza a dos tercios de la población global total.

Figura 9: Porcentaje de penetración de dispositivos móviles a nivel mundial

Usuarios de comercio electrónico en 2019

Se termina el análisis con los datos de los estudios de Perspectivas del Mercado Digital de Statista, que muestran que los consumidores a través de E-comerce son 2.818 millones y el gasto en comercio electrónico se estima superior a los 1,78 billones de dólares.

Estado de las TIC y uso de redes sociales en el ECUADOR

Según datos del portal Datareportal para enero de 2019 (DATAREPORTAL, 2019) El Ecuador posee 16,98 millones de personas; de estos 14,77 millones son suscriptores de telefonía móvil celular,

existen 13,48 millones de usuarios de Internet, de estos 12,35 millones mantienen cuentas en redes sociales y de estos al menos 11 millones usan redes sociales.

Existen otras perspectivas del número de usuarios de Internet para el Ecuador, así, la UIT en su informe de uso de TICs indica que son 9,73 millones; un estudio particular de la compañía World Factbook los ubica en 8,69 millones, los datos del Ministerio de Telecomunicaciones del Ecuador dicen que son 8,67 millones; tomando el dato del MINTEL 8,67 millones de usuarios son 8,67 millones de posibles víctimas de fraudes o delitos a través de Internet, representan un atractivo para individuos que buscan una oportunidad para delinquir y defraudar.

Tabla 7: Sitios Web accedidos por ecuatorianos

Ord	Sitio Web
1	Google.com
2	You Tube.com
3	Elcomercio.com
4	Facebook.com
5	Google.com.ec
6	Live.com
7	Eluniversso.com
8	Ecuavisa.com
9	Thestartmagazine.com
10	Yahoo.com
11	Wikipedia.org
12	Teleamazonas.com
13	Forosecuador.com
14	Blogsport.com
15	Tctelevision.com

Fuente: Ranking de ALEXA

Del ranking se aprecia que Facebook es la principal red social, los sitios web de canales de comunicación sean televisión y periódicos; y los portales financieros privados o del gobierno son los más visitados.

Uso de Redes Sociales en el Ecuador

Con base en la actividad mensual de los usuarios de las principales redes sociales se determina que, de los 12,35 millones de usuarios de redes sociales, 11 millones lo hacen por dispositivos móviles lo que muestra una penetración del 65%.

Tabla 8: Análisis de la composición de estos usuarios de las redes sociales

No. Usuarios	Unidad	Red Social
12	Millones	Facebook
9.9	Millones	Instagram
790	Mil	Twitter
1.1	Millones	Snapchat
12.2	Millones	WhatsApp
2.2	Millones	LinkedIn

Fuente: MINTEL

De las cuentas de usuarios de Facebook el reporte digital de Wearesocial indica que el 92% son mayores de 13 años que pueden ser considerados adultos, Facebook no muestra crecimiento desde el año 2018, el 48% de los usuarios son mujeres y el 52% son hombres. En el caso de Instagram solamente el 30% son adultos y el 55% mujeres y 45% hombres.

Uso de Telefonía Móvil Celular

Con base en el número de líneas celulares 15,54 millones según el MINTEL que muestran una penetración de 87% casi en el rango de los países desarrollados, de estas:

Tabla 9: Subdivisión de la penetración de telefonía celular

1	74%	Son Prepago
2	66%	Usuarios con acceso a Internet
3	51%	Mantienen una cuenta en el sistema financiero bancario
4	8.70%	Tienen una tarjeta de crédito
5	9.70%	Hacen compras en línea
6	4.10%	Acceden a portales de comercio electrónico

Fuente: MINTEL

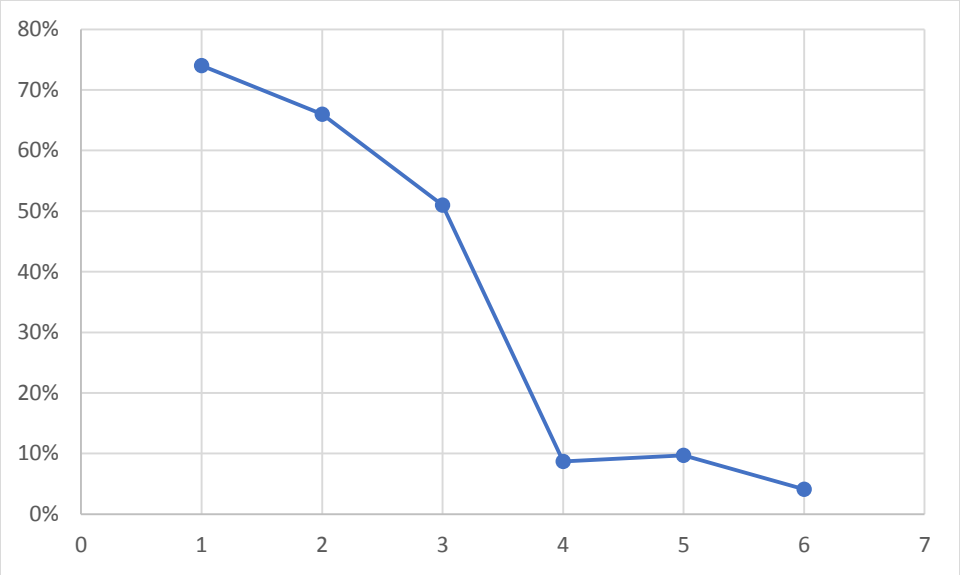


Figura 10: Porcentaje de las características de telefonía móvil

Con estos datos se vuelve a evidenciar que se las aptitudes para manejo de Internet son bajas la posibilidad de ser víctima de delitos a través de TICs es alta.

La Importancia de la Prueba Digital en un Proceso Legal

Se entiende por Prueba digital "Toda información con valor probatoria que es almacenada o transmitida de forma digital o binaria". La aportación de una **prueba digital** en cualquier juicio es cada vez más habitual: comentarios en redes sociales, videos y fotografías, grabaciones de videovigilancia, mensajería instantánea, correos electrónicos, archivos de discos externos, registros (logs) de sistemas informáticos de equipos electrónicos, principalmente. Pero esta gran variedad de fuentes probatorias debe tener acceso al proceso judicial para convertirse en prueba.

Bendinelli, Maximiliano en su artículo "Delitos Informáticos: La Importancia de la Prueba Digital en el Proceso Judicial" (Bendinelli, 2014) claramente expone que, ante el crecimiento constante de las TICs, y el "boom" del Internet al que acceden adultos, jóvenes adolescentes y niños con un solo clic; solamente la educación y la responsabilidad en el uso que se hace de la tecnología y del Internet resultan fundamentales para formar usuarios conscientes de estos peligros.

El uso que se les ha dado, tanto para cometer delitos como para ser utilizados como "medios para", ponen en cuestión todo lo que han habilitado y permitido de las TICs.

Cuando hablamos de delitos informáticos o aquellos cometidos utilizando directa o indirectamente un medio tecnológico, se supone que este medio tecnológico y las evidencias que dejan su uso son pruebas que se puede utilizar para probarlos.

Se entiende por prueba digital a los datos que constan en formato electrónico y que constituyen elementos de prueba, comprendiendo las etapas de extracción, procesamiento e interpretación.

Se requiere un enfoque tecnológico para entender las características de los medios utilizados, y un análisis técnico-jurídico que determine cómo obtener la evidencia, cómo presentar la prueba, cómo interpretarla, y cómo relacionarla con los hechos o actos jurídicos materia de juicio.

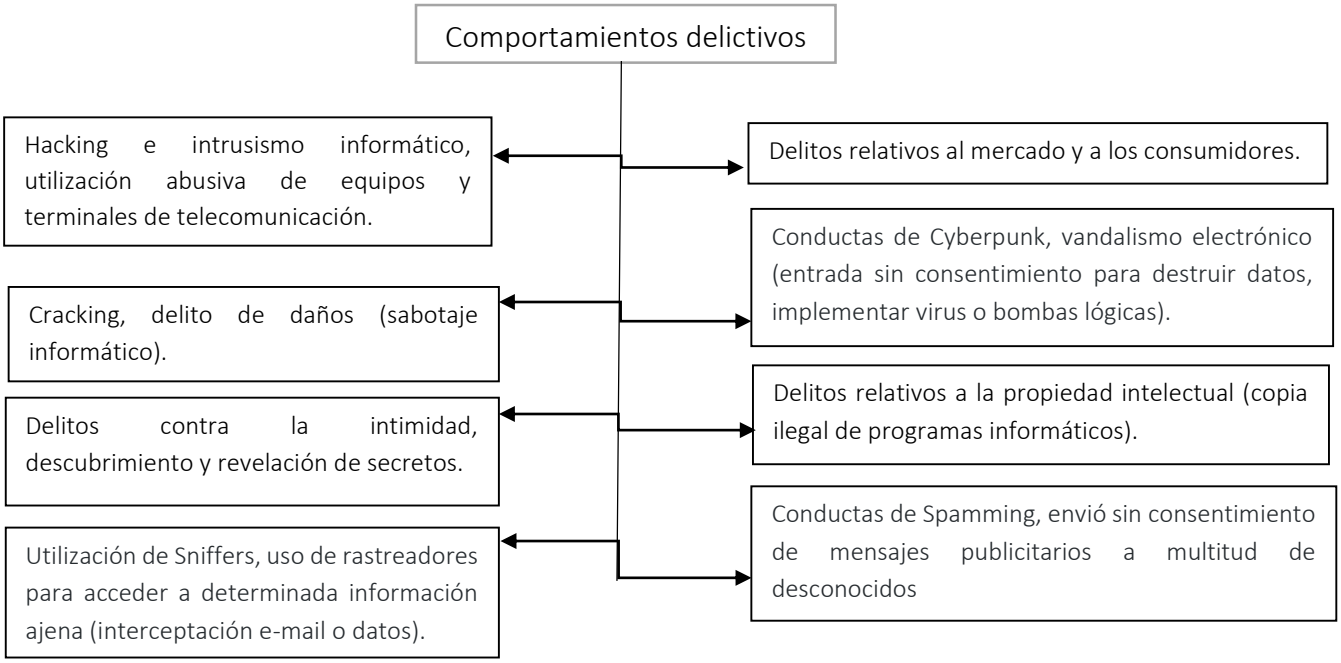
En resumen, puede considerarse a la evidencia digital como un tipo de prueba física en donde sus datos pueden ser recolectados, almacenados y analizados con herramientas informáticas forenses y técnicas especiales.

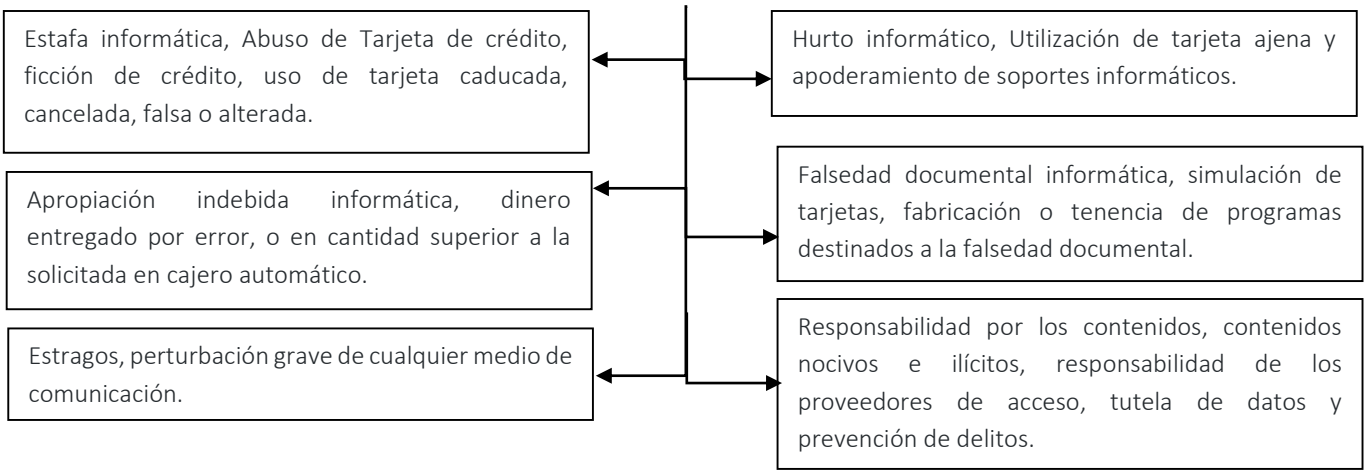
La preponderancia que tiene la prueba o evidencia digital para esclarecer un delito depende de la vinculación que tenga con un caso en particular. Esta puede provenir de un delito informático o de un delito que se cometió utilizando de manera directa o indirecta con algún medio tecnológico (Aranzadi, 2012).

Si la evidencia fue presentada de manera correcta y su cadena de custodia no fue alterada, puede llegar a ser crucial para resolver cualquier clase de delitos.

Pero muchas veces se encuentran algunos inconvenientes a la hora de demostrar o aclarar un hecho, justamente por los problemas que se generan al momento de tipificarlo correctamente, de allí que el Perito Informático debe ser muy cuidadoso y cumplir con los proceso y protocolos que establece la informática forense y la normativa jurídica de cada país, para que no se contamine la evidencia digital y pueda ser considerada prueba en un Juicio.

El informe pericial es muchas veces una prueba importante en el juzgamiento de comportamientos delictivos.





Para ayudar en el juzgamiento de estos delitos el Perito Informático debe ayudar a:

1. Identificar al emisor.
2. Ubicar los rastros que dejó el emisor como la dirección electrónica, dirección IP del computador utilizado, funciones de un usuario en un sistema, etc.
3. Identificar domicilio de los dispositivos involucrados (servidores, computadores).
4. Ayudar a identificar al autor.

En los capítulos siguientes se tratará de conceptualizar los delitos informáticos, sus tipificaciones y la importancia de la informática forense y por ende del Perito informático en el juzgamiento de los delitos especificados anteriormente y otros delitos cometidos con el uso de TICs.

CAPÍTULO 3: Los Delitos Informáticos

Como se expuso en el capítulo introductorio, en cada país se usan definiciones distintas sobre el tema de delitos informáticos. Sin embargo, han surgido esfuerzos de expertos y de organizaciones como la ONU, UNESCO, UIT que buscan proponer la universalidad de delitos relacionados con la tecnología, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas a la legislación de cada país.

Sin embargo, al consultar bibliografía de diferentes fuentes, Carlos Sarzana, indica que los crímenes a través de computadora comprenden "Cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo" (Conde O'Donnell & González P., 2009). María de la Luz Lima conceptualiza que el "delito electrónico", en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el "delito informático", es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin. (Conde O'Donnell & González P., 2009)

Acurio en su artículo Delitos Informáticos: Generalidades (Acurio, Delitos Informáticos, 2017), señala que determinados enfoques subrayarán que el delito informático, más que una forma específica de delito supone una pluralidad de modalidades delictivas vinculadas, de algún modo con los computadores, y a este respecto dice que Romeo Casanoba señala que el término Delito Informático debe usarse en su forma plural, en atención a que se utiliza para designar una multiplicidad de conductas ilícitas y no una sola de carácter general. Se hablará de delito informático cuando nos estemos refiriendo a una de estas modalidades en particular.

Por lo que prefiere delimitar el contenido de los delitos informáticos denominándolos Delincuencia Informática y la define como "Delincuencia informática es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera".

Conceptualización de Delito Informático

Como se ha presentado anteriormente el término "delito informático" en sí no se presta para una sola definición, y probablemente es mejor considerarlo como un conjunto de actos o conductas, y no como un solo acto. No obstante, el contenido básico del término puede describirse al menos para los fines de este estudio, con una lista no exhaustiva de actos que constituyen al delito informático y que se expondrán más adelante y no con la conceptualización que hace el Código Integral Penal.

Por otro lado, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa a la computadora o un equipo tecnológico, tales como "delitos informáticos", "delitos electrónicos", "delitos relacionados con la computadora", "crímenes tecnológicos", “delitos telemáticos”.

Analizando las definiciones antes mencionadas por diversos autores se ha optado usar el término “delito cibernético” y para el presente estudio lo conceptualizamos como: todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal ecuatoriano, que hacen uso indebido de cualquier medio Informático ya sea como medio o como fin, implicando actividades criminales.

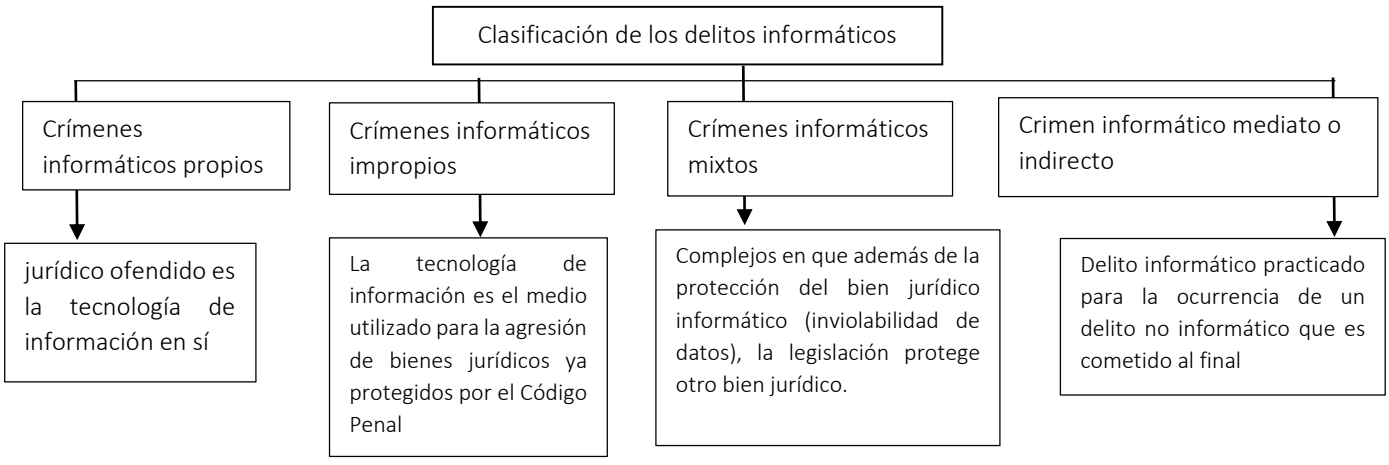
Por ello, probablemente es mejor entender el término “delito cibernético” como un término técnico usado en este estudio y no su definición jurídica.

Clasificación de los delitos cibernéticos.

Aunque no existe una definición universal única de delito cibernético, la aplicación de la ley en los diversos países generalmente hace una distinción entre dos tipos principales de delitos relacionados con Internet (INTERPOL, 2018):

- Ciberdelito avanzado (o crimen de alta tecnología): ataques sofisticados contra hardware y software de computadoras;
- Ciberdelito habilitado: corresponde a muchos delitos 'tradicionales' que han tomado un nuevo giro con la llegada de Internet, tales como delitos contra los niños, los delitos financieros e incluso el terrorismo.

Damásio de Jesus e José Antônio Milagre clasifican a los delitos informáticos de la siguiente forma:



El doctor Jorge Zabala en su estudio “Delitos Informáticos en el Ecuador”, (Baquerizo, 1998), indica que existen dos tipos de delitos informáticos: Delitos computacionales y delitos informáticos. Dice

que el simple hecho de poder diferenciar los delitos computacionales con los informáticos ha provocado una seria confusión al momento de penalizar este tipo de conductas y los define así:

1. Delitos computacionales: Son conductas delictivas que se cometen a través de máquinas conectadas a redes locales, nacionales y globales, con la finalidad de afectar al patrimonio de las personas como por ejemplo cuando tratan de sustraerse bienes, en este caso dinero de cuentas bancarias; o que quieran lesionar el derecho a la intimidad de las personas y el honor.
2. Delitos informáticos: A diferencia de los delitos computacionales estas conductas se atacan entre sí mismo, el daño es directamente al software, o sea el ataque es precisamente de forma lógica más no de forma física, por ejemplo: la intromisión de virus, el acceso prohibido a un computador o a datos restringidos en una red.

Para este trabajo de titulación se acepta la clasificación del doctor Zabala que va en concordancia con la clasificación de INTERPOL, por lo que se clasificará los delitos cibernéticos, como se conceptualizó de la siguiente manera:

1. Delitos Informáticos: Aquellos en que el bien jurídico mira hacia el propio sistema de tratamiento automatizado o los datos contenidos en él. Tales como: Hacking, Web Defacing, Apropiación de Información o Espionaje Informático, Botnet, Denegación de Servicios DDOS, Phishing y Pharming, CriptoLocker y Ransomware
2. Delitos Computacionales: Aquellos ilícitos tradicionales en que la tecnología ha sido utilizada como parte de una especial forma de comisión de otros delitos, fraudes o infracciones, tales como: Ingeniería social, Estafa, Usurpación de nombre, Amenazas, Injurias, Calumnias, Pornografía Infantil, Falsificación, Robo de perfiles, Ciberbulying, Sexting, Difamaciones, Porno Venganza, Falsificación de documentos, Skimming.

Tanto los delitos computacionales como los informáticos tienen una relación directa con el uso de las TICs, y como éstas a su vez provocan un impacto delincuencial de alta magnitud a la sociedad; por lo que un estudio como el propuesto contribuye a combatir este problema.

Características de los Delitos Cibernéticos

Según Leonardo Sinchiguano (Leonardo, 2014) en su tesis presenta como características de los delitos informáticos (entiéndase delitos cibernéticos):

- Sólo una determinada cantidad de personas pueden llegar a cometerlos.
- Provocan pérdidas económicas.
- Son muchos los casos y pocas las denuncias.
- Presentan grandes dificultades para su comprobación, por su carácter técnico.
- Delitos difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas.
- Tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución.

Se puede decir entonces que por la forma en que se ejecutan los delitos cibernéticos pueden caracterizarse por:

- Son delitos difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas.
- Son actos que pueden llevarse a cabo de forma rápida y sencilla.
- No se requiere de presencia física para cometerlos.
- Se pueden ocultar por largos períodos de tiempo.
- Se requieren personas con conocimientos técnicos para ejecutarlos.

Tipos de delitos Cibernéticos

Los delitos cibernéticos abarcan una gran variedad de modalidades como se mencionan en la web de la INTERPOL (INTERPOL, 2018) y se enlista a continuación:

- Ataques contra sistemas y datos informáticos.
- Usurpación de la identidad.
- Distribución de imágenes de agresiones sexuales contra menores.
- Estafas a través de Internet.
- Intrusión en servicios financieros en línea.
- Difusión de virus.
- Botnets, redes de equipos infectados controlados por usuarios remotos.
- Phishing, adquisición fraudulenta de información personal confidencial.

Sin embargo, no son los únicos, también existen riesgos relacionados con el uso de las redes sociales y acceso a todo tipo de información tales como:

- Acceso a material inadecuado (ilícito, violento, pornográfico, etc.).
- Adicción - Procrastinación (distracciones para los usuarios).
- Problemas de socialización.
- Robos de identidad.
- Acoso (pérdida de intimidad).
- Sexting (manejo de contenido erótico).
- Ciberbullying (acoso entre menores por diversos medios: móvil, Internet, etc.).
- Cibergrooming (método utilizado por pederastas para contactar con niños y adolescentes en redes sociales o salas de chat).

Los delincuentes con conocimientos técnicos desarrollan herramientas que les permitan llevar a cabo sus objetivos, a este tipo de herramientas se les conoce como Malware. En Internet, este tipo de amenazas crecen y evolucionan día a día, por lo que las compañías de antivirus trabajan

continuamente en sus laboratorios, ofrecen soluciones dirigidas a diferentes tipos de usuarios tales como hogares y oficinas, o al sector industrial y empresarial e incluso gobiernos.

Un ejemplo de la protección que se ofrece es la siguiente lista de las principales categorías de riesgo para las cuales la firma antivirus alemana AVIRA (Avira Operations GmbH & Co. KG., 2019) ofrece protección:

- Adware (muestra contenido publicitario en las actividades del usuario).
- Spyware (Recopila datos personales y los envía a un tercero sin consentimiento del usuario) Aplicaciones de origen dudoso (programas que pueden poner en riesgo el equipo).
- Software de control backdoor (Permiten el acceso remoto al equipo).
- Ficheros con extensión oculta (Malware que se oculta dentro de otro tipo de archivo para evitar ser detectado).
- Suplantación de identidad (phishing).
- Programas que dañan la esfera privada (Software que mermar la seguridad del sistema).
- Programas broma Juegos (distracción en el entorno laboral).
- Software engañoso (hacen creer el usuario que esta vulnerable y lo persuaden para comprar soluciones).
- Utilidades de compresión poco habituales (archivos generados de manera sospechosa).

Riesgo Social

Las relaciones sociales han sido un punto clave en la vida de las personas. Tener la facilidad de contactar con cualquier persona en cualquier parte del mundo ha contribuido a la globalización y al mismo tiempo ha generado una serie de riesgos.

Tabla 10: Conductas identificadas que ponen en riesgo la integridad de los usuarios

Ciberbullying	Acoso que se da entre menores mediante insultos, humillaciones, amenazas a través de redes sociales u otros medios de comunicación. Si bien el Bullying se inició en las escuelas y parques; hoy día se ha expandido a las redes sociales donde no existe la vigilancia de los padres.
Sexting	El término hace referencia al uso de la telefonía móvil para mantener charlas de índole sexual, donde voluntaria o involuntariamente se genera contenido que implique una situación erótica o sexual.
Acceso a Material Inadecuado	A pesar de que los proveedores de Internet siempre buscan mantener fuera de los resultados el contenido no apto para el usuario, existe otra parte de la red. Conocida como Deep Web (Internet profunda) que es el conjunto de sitios que contienen material potencialmente peligroso para el usuario, no solo de índole sexual, también existen, videos Snuff (grabaciones de asesinatos, violaciones, torturas y otros crímenes reales), mercado negro

	online (tráfico de armas, drogas, trata de personas), contratación de asesinos, no existen límites para la gravedad del contenido que se puede encontrar.
Pornografía Infantil	Los pederastas han hecho uso de las tecnologías de la información por las diferentes ventajas facilitan la realización de esta actividad: • Anonimato: La facilidad de cambiar de identidad dentro de foros en Internet dificulta el seguimiento de las acciones de un mismo sujeto. • Cifrado: Herramientas que ofrecen métodos de cifrado (incluso a grado militar) para la información que aseguran que ninguna otra persona tenga acceso, y por tanto pruebas, a menos que se conozca una contraseña. • Dificultad de Rastreo: Si bien es posible obtener cierta información acerca de la fecha de acceso, ubicación y dispositivos utilizados, usuarios avanzados pueden hacer uso de programas con los que se pueden falsear estos registros.
Riesgo Empresarial	En un ambiente donde los riesgos avanzan a gran velocidad como lo es Internet no existen soluciones de seguridad definitivas, por lo que todas las empresas, sin importar el giro, tamaño o ubicación son susceptibles de recibir ataques informáticos.

Todos estos tipos de comportamientos sociales delictivos pueden agruparse en el cometimiento de delitos comunes en la siguiente propuesta para este trabajo:

Tabla 11: Fraude y extorción

Comercio electrónico	Consiste en la compra y venta de productos o de servicios a través de medios electrónicos, tales como redes sociales y otras páginas web.
Banca en línea	Es la banca a la que se puede acceder mediante Internet. Pueden ser entidades con sucursales físicas o que sólo operan a distancia (por Internet o por teléfono).
Phishing	Conocido como suplantación de identidad, es un término informático que denomina un modelo 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.
Pharming	Es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (Domain Name) a otra máquina distinta.

Smishing	Es un nuevo tipo de delito o actividad criminal a base de técnicas de ingeniería social con mensajes de texto dirigidos a los usuarios de telefonía móvil.
Ransomware	Es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado, y pide un rescate a cambio de quitar esta restricción

Tabla 12: Vulnerabilidades de seguridad de sistemas informáticos

Malware	Tipo de software que tiene como objetivo infiltrarse o dañar una computadora, o todo otro sistema de información.
Spam	Se refiere a la publicidad encubierta como artículos o secciones y enlaces externos masivos.
Modificación no autorizada de contenidos	Utilización no autorizada de programas para alterar datos y resultados, u obtener información.
Denegación de servicios (botnet)	Se refiere a un conjunto de equipos infectados, denominados zombis, controlados remotamente por un atacante que pueden ser utilizados individualmente o en conjunto para realizar actividades maliciosas.
Diddling	Se refiere a la modificación no autorizada de los datos de un sistema o solución informática.
Salami Technique	Fraude consistente en realizar pequeñas manipulaciones que, sumadas, alcanzan un gran valor esto se ve en la desviación fraudulenta de centavos en transacciones bancarias o nóminas de empresas.
Bomba lógica (Logic bomb)	Código oculto en un sistema que se ejecuta en determinadas circunstancias, como una fecha o una secuencia de teclas y que genera una serie de acciones generalmente malignas, como bloquear la máquina, anular los sistemas de seguridad o destruir información.
Hacktivismo (un acrónimo de hacker y activismo)	Se entiende la utilización de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos
Data Breach o divulgación de información	Se refiere a la liberación intencional o no de información segura a un entorno inseguro.

Juzgamiento de Delitos Cibernéticos en el Ecuador

Andrés Llangari (Llangari, 2016), en su trabajo de titulación hace una propuesta de identificación de algunos de los delitos cibernéticos y como estos pueden juzgarse aplicando en COIP en el Ecuador, presenta un análisis del COIP identificando los posibles artículos que pueden usarse para juzgar los delitos cibernéticos (informáticos y computacionales) como se presenta a seguir:

Tabla 13: Identificación de delitos cibernéticos y juzgamiento aplicando el COIP en Ecuador

Datos falsos o engañosos (Data Diddling)	
Articulo	Delito
178	Violación a la intimidad
190	Apropiación fraudulenta por medios electrónicos
230	Interceptación ilegal de datos. Inciso Número 1
232	Ataque a la integridad de sistemas informáticos
Manipulación de programas, Malware o los "Caballos de Troya"	
232	Ataque a la integridad de sistemas informáticos. Incisos Números 1 y 2
La técnica del salami (Salami Technique/Rounching Down)	
190	Apropiación fraudulenta por medios electrónicos
231	Transferencia electrónica de activo patrimonial
Falsificaciones informáticas	
178	Violación a la intimidad
186	Estafa. Inciso número 1
231	Transferencia electrónica de activo patrimonial
Manipulación de los datos de salida	
186	Estafa. Incisos números 1 y 2
190	Apropiación fraudulenta por medios electrónicos
230	Interceptación ilegal de datos. Inciso número 3
Pishing	
178	Violación a la intimidad
186	Estafa. Inciso número 1
190	Apropiación fraudulenta por medios electrónicos
212	Suplantación de identidad
230	Interceptación ilegal de datos. Inciso número 2
Bombas lógicas (logic bombs)	
232	Ataque a la integridad de sistemas informáticos. Incisos números 1 y 2
Malware (gusanos)	

190	Apropiación fraudulenta por medios electrónicos
232	Ataque a la integridad de sistemas informáticos. Incisos números 1 y 2
Virus informáticos y Malware	
190	Apropiación fraudulenta por medios electrónicos
232	Ataque a la integridad de sistemas informáticos. Incisos números 1 y 2
234	Acceso no consentido a un sistema informático
Ciberterrorismo	
366	Terrorismo. Número 1
Ataques de denegación de servicio	
190	Apropiación fraudulenta por medios electrónicos
232	Ataque a la integridad de sistemas informáticos. Incisos números 1 y 2
Fuga o violación de datos (Data Leakage)	
178	Violación a la intimidad
229	Revelación ilegal de base de datos
Hurto del tiempo del computador	
229	Revelación ilegal de base de datos
234	Acceso no consentido a un sistema informático
Acceso no consentido (piggybacking) y suplantación de personalidad (impersonation)	
178	Violación a la intimidad
190	Apropiación fraudulenta por medios electrónicos
212	Suplantación de identidad
Llave maestra (superzapping)	
230	Interceptación ilegal de datos. Inciso número 1
232	Ataque a la integridad de sistemas informáticos. Número 1 y 2
234	Acceso no consentido a un sistema informático
Clonación de teléfonos celulares	
190	Apropiación fraudulenta por medios electrónicos
191	Reprogramación o modificación de información de equipos terminales móviles.
192	Intercambio, comercialización o compra de información de equipos terminales móviles.
193	Reemplazo de identificación de terminales móviles
194	Comercialización ilícita de terminales móviles
195	Infraestructura ilícita
212	Suplantación de identidad
232	Ataque a la integridad de sistemas informáticos. Inciso número 1
234	Acceso no consentido a un sistema informático.

Fuente: Análisis de los Delitos Informáticos y de Telecomunicaciones en el Ecuador Bajo las Nuevas Normas Jurídicas

La Universidad Técnica Particular de Loja, presenta la siguiente asociación de artículos del COIP que pueden juzgar los delitos cibernéticos más comunes en el Ecuador:

Tabla 14: Delitos Cibernéticos más comunes en el Ecuador asociados a los artículos del COIP

TIPO DE DELITO	ARTICULO DE COIP APLICABLE
Accesos no Autorizados Fallos y Vulnerabilidades	Art. 178. Violación de la Intimidad Art.190. Apropiación Fraudulenta de Medios Electrónicos Art. 211 Supresión, alteración o suposición de la identidad y estado civil. Art.212 Suplantación de identidad Art. 231 Transferencia electrónica de activo patrimonial. Art.234 Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.
Pornografía Pornografía Infantil	Art.103 Pornografía con utilización de niñas, niños o adolescentes.
Estafas Correos Nigerianos, Loterías, Actualización de Información Bancaria (Pishing)	Art. 190 Apropiación fraudulenta por medios electrónicos. Art. 211 Supresión, alteración o suposición de la identidad y estado civil. Art. 212 Suplantación de identidad
Secuestro, Extorsión Ransomware	Art. 212 Suplantación de identidad
Robo de Identidad Escucha de redes, Pishing	Art. 178 Violación a la intimidad Art. 211 Supresión, alteración o suposición de la identidad y estado civil.
Robo de Información	Art.190 Apropiación fraudulenta por medios electrónicos. Art. 229 Revelación ilegal de base de datos Art. 230 Interceptación ilegal de datos
Código Malicioso Virus, Malware, vulneraciones	Art. 231 Transferencia electrónica de activo patrimonial. Art. 232 Ataque a la integridad de sistemas informáticos
Interrupción del servicio, Denegación de servicio distribuido DDO, DDoS	Art. 232 Ataque a la integridad de sistemas informáticos Art. 233 Delitos contra la información pública reservada legalmente

Utilización No autorizada se servicios Actividades propias, hacktivismo, botnets	Art. 233 Delitos contra la información pública reservada legalmente

Fuente: Universidad Técnica Particular de Loja

Pero además de estas asociaciones del COIP para el juzgamiento de los delitos cibernéticos; existen otros artículos del COIP que a criterio de varios investigadores en el que el autor se suma, involucran las Tecnologías de Información y Comunicaciones (TICs); y que pueden usarse en el juzgamiento caso de ser infringidas. A continuación, se presentan los artículos del COIP pertinentes:

Artículo 104.- Comercialización de pornografía con utilización de niñas, niños o adolescentes.

Artículo 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos.

Artículo 180.- Difusión de información de circulación restringida.

Artículo 211.- Supresión, alteración o suposición de la identidad y estado civil.

La persona que ilegalmente impida altere, añada o suprima la inscripción de los datos de identidad suyos o de otra persona en programas informáticos, partidas, tarjetas índices, cédulas o en cualquier otro documento emitido por la Dirección General de Registro Civil, Identificación y de Cedulación o sus dependencias o, inscriba como propia, en la Dirección General de Registro Civil, Identificación y de Cedulación a una persona que no es su hijo.

Artículo 354.- Espionaje.

La o el servidor militar, policial o de servicios de inteligencia que en tiempo de paz realice uno de estos actos:

1. Obtenga, difunda, falsee o inutilice información clasificada legalmente y que su uso o empleo por país extranjero atente contra la seguridad y la soberanía del Estado.
2. Intercepte, sustraiga, copie información, archivos, fotografías, filmaciones, grabaciones u otros sobre tropas, equipos, operaciones o misiones de carácter militar o policial.

Artículo 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.

Artículo 231.- Transferencia electrónica de activo patrimonial

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

Artículo 229.- Revelación ilegal de base de datos

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

Como se aprecia, tanto la legislación ecuatoriana como la academia han hecho sus esfuerzos para identificar los delitos cibernéticos y tipificarlos para un mejor juzgamiento de estos. Sin embargo, no se valora una acción coordinada, por lo que es necesario que instituciones como la Asamblea Nacional, responsable de la promulgación de leyes, haga un esfuerzo por normar claramente este tipo de nuevos delitos. Con el fin de contribuir a este esfuerzo este trabajo de titulación ha considerado importante valorar lo que actualmente pasa en el juzgamiento de este tipo de delitos, a través de un trabajo de campo, para lo que se solicitó a las instituciones responsables de la investigación y del juzgamiento se proporcione el número de noticias de delitos y en número de causas juzgadas, encontrando lo siguiente:

Tabla 15: Número de Causas Ingresadas y Resueltas en 2017 y 2018

PROVINCIA	CAUSAS INGRESADAS 2017	CAUSAS INGRESADAS 2018	CAUSAS RESUELTAS 2017	CAUSAS RESUELTAS 2018
AZUAY	109	84	102	76
BOLIVAR	40	33	25	37
CAÑAR	65	32	67	41
CARCHI	12	20	9	18
CHIMBORAZO	103	98	95	89
COTOPAXI	40	52	36	42
EL ORO	115	117	80	87
ESMERALDAS	72	58	48	40
GALAPAGOS	8	7	5	5
GUAYAS	352	314	249	257
IMBABURA	52	37	47	44
LOJA	67	58	35	50
LOS RIOS	86	61	78	65
MANABI	125	140	97	111
MORONA SANTIAGO	22	28	19	28
NAPO	21	21	18	10

ORELLANA	22	24	20	15
PASTAZA	11	8	18	8
PICHINCHA	327	305	244	267
SANTA ELENA	22	12	20	24
SANTO DOMINGO DE LOS TSACHILAS	42	35	34	38
SUCUMBIOS	42	16	37	17
TUNGURAHUA	79	75	77	77
ZAMORA CHINCHIPE	13	7	9	8
Total	**1.847**	**1.642**	**1.469**	**1.454**

Fuente: Sistema Automático de Trámites Judiciales (SATJE)

En el caso de los delitos más comunes asociados al uso de TICs, las estadísticas en el Ecuador para los años 2017 y 2018 muestran los siguientes datos:

Tabla 16: Delitos Comunes Asociados al uso de TICs

Delito	Causas Ingresadas 2017	Causas Ingresadas 2018
103 pornografía con utilización de niñas, niños o adolescentes, INC.2	1	-
103 pornografía con utilización de niñas, niños o adolescentes, INC.3	1	-
103 pornografía con utilización de niñas, niños o adolescentes	-	1
103 pornografía Infantil, INC.1	22	10
178 violación a la intimidad de datos	69	98
179 revelación de secreto	-	1
186 estafa, INC.1	1256	1124
186 estafa, INC.2	19	14
186 estafa, INC.3	25	8
186 estafa, INC. Final	3	3
186 estafa, INC.1	-	2
186 estafa, NUM.1	107	52
186 estafa, NUM.2	5	7
186 estafa, NUM.3	3	5
186 estafa, NUM.4	11	17
186 estafa, NUM.5	12	4
190 apropiación Fraudulenta por Medios Electrónicos, INC.1	25	16
190 apropiación Fraudulenta por Medios Electrónicos, INC.2	4	6
191 reprogramación o modificación de información de equipos	6	-
193 reemplazo de identificación de terminales móviles	1	-
194 comercialización ilícita de terminales móviles	1	7

195 infraestructura Ilícita	1	3
211 supresión, alteración o suposición de la identidad o estado civil	15	4
211 supresión, alteración o suposición de la identidad o estado civil INC.2	1	1
212 suplantación de Identidad	248	241
229 revelación ilegal de Base de datos	-	1
230 interceptación ilegal de datos - NUM.1	1	1
230 interceptación ilegal de datos - NUM.2	1	-
231 transferencia electrónica de activo patrimonial	3	3
231 transferencia electrónica de activo patrimonial - INC.FINAL	-	-
232 ataque a la integridad de sistemas informáticos, INC.1	-	5
232 ataque a la integridad de sistemas informáticos, INC.FINAL	-	-
233 delitos contra la información pública reservada	3	-
234 acceso No consentido a un sistema informático o telemático	2	3
366 terrorismo, INC.1	1	1
266 terrorismo, NUM.2	-	3
366 terrorismo, NUM.4	-	1
TOTAL	1847	1642

Fuente: Sistema Automático de Trámites Judiciales (SATJE)

En el caso de la provincia de Pichincha que es de interés para este estudio, se presentan los siguientes datos.

Tabla 17: Número de Causas Ingresadas en la Provincia de Pichincha en 2017 y 2018

Delito	Causas Ingresadas 2017	Causas Ingresadas 2018
103 pornografía Infantil, INC.1	1	0
178 violación a la intimidad de datos	2	0
186 estafa, INC.1	1	0
212 suplantación de Identidad	4	2
103 pornografía Infantil, INC.1	2	0
103 pornografía con utilización de niñas, niños o adolescentes, INC.3	1	0
178 violación a la intimidad de datos	7	11
186 estafa, INC.1	180	197
186 estafa, INC.2	6	6
186 estafa, INC.3	5	2
186 estafa, INC. Final	1	0
186 estafa, NUM.1	20	9

186 estafa, NUM.2	4	1
186 estafa, NUM.3	1	1
186 estafa, NUM.4	1	1
186 estafa, NUM.5	3	1
190 apropiación Fraudulenta por Medios Electrónicos, INC.1	3	0
190 apropiación Fraudulenta por Medios Electrónicos, INC.2	1	3
211 supresión, alteración o suposición de la identidad o estado civil	1	0
212 suplantación de Identidad	82	63
230 interceptación ilegal de datos - NUM.1	0	1
230 interceptación ilegal de datos - NUM.3	1	0
232 ataque a la integridad de sistemas informáticos, INC.1	0	2
234 acceso No consentido a un sistema informático o telemático	0	2
186 estafa, INC.1	0	1
186 estafa, NUM.1	0	1
366 terrorismo, NUM.4	0	1
TOTAL	327	305

Fuente: Sistema Automático de Trámites Judiciales (SATJE)

CAPÍTULO 4: La Investigación de los Delitos Cibernéticos

Una vez que se ha presentado cómo el constante crecimiento de las TICs ha proliferado el cometimiento de nuevos delitos, en este capítulo se pretende presentar las formas en que se hace la investigación de los delitos que involucran TICs en los organismos policiales y de gobiernos a nivel global y en el Ecuador.

Informática Forense

La informática forense es la práctica de recopilar, identificar, analizar e informar sobre datos digitales de forma legalmente admisible. se puede usar en la detección y prevención de delitos y en cualquier disputa donde las pruebas se almacenan digitalmente. (Krause, 2019)

Según el FBI, la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional. (FBI, 2018). La informática forense se basa en analizar las evidencias electrónicas sin alterar el estado del sistema.

Pericia Informática

La pericia informática es el procedimiento por el cual un especialista en el campo de tecnología hace uso tanto de sus conocimientos como de herramientas de TI para generar evidencia que aporte a un juicio.

Perito

Es el experto en una materia, capaz de aportar a juez conocimientos que no posee, con el fin de darle los respectivos detalles y aclararle la situación al juez, quien es el encargado de determinar las responsabilidades civiles, administrativas y penales.

Perito informático

Es un Perito especializado en el área de Tecnologías de la Información (TI) que de acuerdo con el tema requerido puede ser seleccionado según su competencia y experiencia para una labor de análisis y aportar con pruebas en un Juicio, se considera un ayudante o asesor del Juez.

Existen actualmente algunas metodologías en el campo de sistemas de información para realizar un correcto procedimiento en la investigación. Sin embargo, se ha recolectado los procesos más recomendados por los Peritos.

Proceso del Protocolo de Análisis Forense (basado en 7 fases)

Este proceso o método de investigación se basa en clasificar las evidencias en tres etapas esenciales, estas son:

1. Técnica: Contribuye en la búsqueda de indicios y bitácoras de auditoría.
2. Pericial: El Perito examina y transforma la evidencia en medios de prueba.

3. Legal y de Comunicación: El asesor legal denuncia el delito apoyado en el informe pericial.

La bibliografía y documentación consultada indican que se está trabajando en la estandarización de los procedimientos forenses informáticos, a fin de alinearlos y facilitar la comunicación y trabajo cooperativo entre otros organismos de investigación y laboratorios criminalísticos (Cobarrubias, 2009).

Pasos forenses relativos a la informática:

Identificación y descripción de la evidencia.

1. Fijación fotográfica, planimétrica y digital con Integridad mediante código Hash.
2. Levantamiento.
3. Protección y resguardo criptográfico.
4. Análisis pericial asistido y protegido de evidencia electromagnética.
5. Interpretación y generación de conclusiones.
6. Presentación de la evidencia.

Dicho esto, es necesario seguir estos pasos dado que la evidencia puede alterarse y llegar al punto de ser inútil en caso de ser manipulada con fines maliciosos.

El Principio de Intercambio o Transferencia de Locard

Edmon Locard fue un francés pionero de la criminalística a principios del siglo XX ya en esa época su propuesta consistía en la siguiente apreciación: “Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto" (Gutiérrez & Zuccardi, 2006). Este principio ha permitido obtener significantes evidencias en lugares insospechados desde esos tiempos, como por ejemplo huellas dactilares, sangre o cabello.

Básicamente, su propuesta plantea que un criminal siempre deja un rastro en la escena del crimen, por esto la informática ha utilizado este principio como un apoyo a la gestión de la recolección de las evidencias digitales dejadas en un sistema informático después de realizar un acto ilícito.

Evidencia digital

La evidencia digital son los datos o información que se obtienen de los equipos tecnológicos, para ser analizadas y presentarlos posteriormente como evidencia.

La evidencia digital debe ser copiada exactamente para asegurar que su contenido no ha sido modificado. Con las herramientas de análisis forense se puede determinar que la copia es exacta, por ejemplo: los algoritmos MD5 y SHA1 para generar el archivo HASH.

La evidencia digital es usada en la investigación y el juzgamiento de diversos conflictos, denuncias, delitos, fraudes, tales como los descritos en el capítulo anterior y tipificados en la legislación del Ecuador.

Dicho esto, no es de sorprenderse que la evidencia digital sea considerada como el componente fundamental de cualquier investigación. Dentro de sus desventajas, esta evidencia puede ser: eliminada, copiada, alterada, volátil, duplicada y de esta forma ser anulada como prueba en un Juicio. Así lo refiere Serna, Rivera & Morales "Un obstáculo para aceptar la evidencia digital es la carencia en los códigos procesales penales de normas especializadas destinadas a salvaguardar la cadena de custodia y admisibilidad de la evidencia digital" (Serna, Rivera, & Morales, 2012).

Existen mecanismos tecnológicos que permiten sustentar la solidez de la evidencia y sus alteraciones, para esto el Perito Informático debe apoyarse en los sistemas de correlación de eventos, logs de auditoría, sistemas de detección de intrusiones, registro de autenticación, autorización y estampas de tiempo para sustentar sus apreciaciones.

Las barreras geográficas se han roto con el avance tecnológico, muchas veces varias naciones están involucradas en el juzgamiento de un delito cibernético. Por esta razón, es importante que existan mecanismos sólidos para el manejo de evidencia digital. Así mismo, es necesario que el Perito informático utilice un lenguaje comprensible y didáctico que le permita al juez entender los procedimientos y resultados de la investigación forense digital.

Manual de Manejo de Evidencias Digitales y Entornos Informáticos de la Fiscalía General del Ecuador

La Policía Judicial, la Fiscalía General del Estado y el Consejo de la Judicatura, que son las entidades encargadas de la justicia en el Ecuador deben especializarse y capacitarse en estas nuevas áreas en donde las TICs se convierten en herramientas necesarias en auxilio de la Justicia y la persecución de delito y el delincuente (Acurio, 2009).

Para cumplir esta aspiración planteada por el Doctor Acurio, La Fiscalía General del Ecuador autorizó el Manual de manejo de evidencias digitales y entornos informáticos, con el fin de ser una guía para los funcionarios de las instituciones mencionadas anteriormente en caso de encontrar en una escena del delito dispositivos Informáticos o electrónicos que estén relacionados con el cometimiento de una infracción de acción pública.

Principios básicos planteados por el manual:

1. El funcionario debe acudir acompañado al lugar de los hechos.
2. No debe efectuarse ninguna acción que altere la información que esta almacenada en los sistemas informáticos o medios magnéticos.
3. Solo una persona capacitada puede tener acceso a la información original almacenada en el sistema informático objeto de la investigación.
4. Se debe llevar una bitácora de todos los procesos adelantados con relación a la evidencia digital.
5. El fiscal del caso es el encargado de garantizar el cumplimiento de la ley. Así mismo, como el acceso a las personas pertinentes a la información.

Es necesario identificar cuando el hardware o software sirven como evidencia digital y el procedimiento que se debe seguir dependiendo la situación en la que haya sido usado. Es decir, cada tipo de evidencia tiene un procedimiento adecuado para ser tratada.

El hardware y la información son clasificados de tres maneras dependiendo la forma en la que fueron usados en el cometimiento del crimen. Estas son: mercancía ilegal, como instrumento y como evidencia.

La evidencia digital es clasificada en tres grupos:

- Sistemas de computación abiertos.
- Sistemas de comunicación.
- Sistemas convergentes de computación.

Responsabilidades de los investigadores que llegan primero a la escena del crimen:

- Observar y establecer los parámetros de la escena del delito.
- Iniciar las medidas de seguridad.
- Facilitar los primeros auxilios.
- Asegurar físicamente la escena y las evidencias.
- Entregar la escena del delito.

Las evidencias encontradas permiten hacer una reconstrucción del suceso y observar que fue lo sucedido. Existen tres clases de reconstrucción:

- Reconstrucción Relacional: Se relaciona los objetos presentes con un objeto de la escena del crimen.
- Reconstrucción Funcional: Se determina la función de cada objeto en la escena.
- Reconstrucción Temporal: Se determina indicios para crear una línea de tiempo del cometimiento.

El manual indica detalladamente qué hacer en caso de encontrarse con un dispositivo electrónico y no esté presente un técnico para controlar la situación adecuadamente. Además, las repercusiones que tendría en caso de ser manipulados incorrectamente. Es más, guía como deben ser las buenas prácticas con el manejo de hardware.

Sin embargo, a pesar de la existencia de este manual, como se demostrará más adelante, el incumplimiento de esta norma es general en la mayoría de las denuncias u Juicios donde se pretende usar la evidencia digital.

En las actividades cotidianas de las personas el uso de las comunicaciones electrónicas a través de mensajes de texto, mensajes en redes sociales y especialmente en correos electrónicos son evidencias muchas veces usadas en las denuncias y juicios, por lo que se dedicará un tiempo a describir como estas comunicaciones pueden ayudar en la investigación de los delitos.

El Código Orgánico Integral Penal (COIP) enseña cómo manejar los contenidos digitales, de la siguiente manera:

Artículo 500.- Contenido Digital

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 (Asamblea Nacional, 2014).

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.

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.

De la Investigación bibliográfica y documental, no se encuentra que el Ecuador haya reglamentado el uso de alguna metodología que guíe la investigación de delitos cibernéticos, las mayores aproximaciones se dan en la aplicación de normas de Organismos internacionales como la Organización Internacional de Normalización ISO o de otros países que ya han establecido sus metodologías, las que se considera de utilidad para este estudio y se presentan a seguir.

Metodologías Internacionales

Los estándares ISO se crearon con el fin de minimizar los tiempos de investigación e implementación de herramientas. Así, mejorando el proceso de investigación forense al más viable

posible. A continuación, se presenta una revisión de las regulaciones existentes para el correcto manejo de evidencia digital.

Se parte del hecho que la información debe ser protegida por los mismos sistemas que la procesan, éste es uno de los principales objetivos en un proceso investigativo. Para poder manejar toda la información y para que esta pueda ser empleada en un proceso judicial, es necesario tener métodos donde cada proceso esté documentado con bases de seguridad y análisis de riesgos.

Para cumplir con los requerimientos existen estándares que guían el manejo de la seguridad de la información, identificación de riesgos e implementación de controles de seguridad (SGSI).

La ISO/IEC 27000 es un conjunto de estándares que incluyen las mejores prácticas en el área de la seguridad de la información. Dentro de esta familia de estándares, existen estándares específicos que pueden ser añadidos a las prácticas de la informática forense. Nos referiremos a las normas 27037 y 27042 por ser las que incluyen las fases de un proceso pericial.

Tabla 18: Estándares que pueden relacionarse con las prácticas forenses

ISO/IEC 27041 (2015)	Orientación para asegurar la idoneidad y adecuación del método de investigación del incidente.
ISO/IEC 27037 (2012)	Directrices para identificación, recolección, adquisición y preservación de la evidencia digital.
ISO/IEC 27017 (2015)	Código de buenas prácticas para el control de la seguridad de la información para servicios en la nube.
ISO/IEC 27050 (2017)	Código de práctica para el descubrimiento electrónico.
ISO/IEC 27042 (2015)	Directrices para el análisis e interpretación de la evidencia digital.

Fuente: International Organization for Standardization

ISO/IEC 27037: Directrices para la Identificación, Recolección, Adquisición y Preservación de la Evidencia Digital.

Esta ISO proporciona guías para actividades específicas en el manejo de evidencia digital, dichas actividades hacen referencia a la identificación, recolección, adquisición y preservación de evidencia digital potencial.

Figura 11: Etapas de la norma ISO 27037:2012

Fuente: Metodología para la recolección de evidencia forense generada durante la utilización de aplicaciones desplegadas en entornos web (Coronel, 2018)

Provee guías para:

- Medios de almacenamiento usados en computadores estándares.
- Dispositivos móviles.
- Sistemas móviles de navegación.
- Computadores estándares y conexiones de red.
- Redes basadas en los protocolos TCP/IP y otros.

ISO/IEC 27042: 2015 Directrices para el análisis e interpretación de la evidencia digital

Según especifica (IT-Security, 2013) la Organización de Estándares Internacionales (ISO) con el afán de dar respuesta las necesidades informáticas forenses crearon la ISO 27042:2015, la cual mediante un marco de buenas prácticas asegura que las actividades realizadas en las investigaciones forenses se ejecutan de manera equivalente. Por ello, ISO/IEC (2015) expresa que la ISO 27042:2015 está relacionada particularmente al análisis forense.

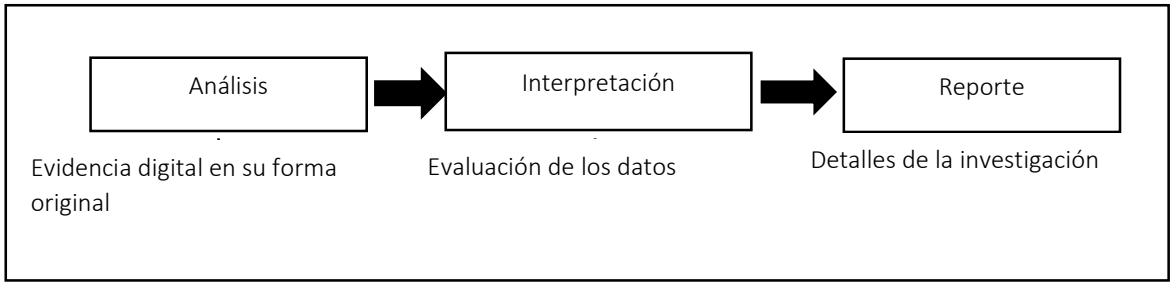


Figura 12: Etapas de la norma ISO 27042:2015

Fuente: Fuente: International Organization for Standardization

La norma provee guías en el análisis y la interpretación de la evidencia digital, de forma que se logre garantizar o abordar cuestiones de continuidad, validez, reproductibilidad y repetitividad. Contiene, además, buenas prácticas para la selección, diseño e implementación de un proceso analítico y recoger suficiente información que permita que dichos procesos puedan ser sometidos a escrutinios independientes cuando sea necesario.

Metodología del Departamento de Justicia de Estados Unidos

El reporte del Instituto Nacional de Justicia (NIJ, 2004) del Departamento de Justicia de los Estados Unidos indica que esta guía fue creada para el uso de los encargados de hacer cumplir la Justicia y otros miembros de la comunidad que sean responsables del examen de las pruebas digitales. Esta metodología incluye cuatro etapas en cada una de ellas se describen los pasos necesarios para realizar un análisis forense informático y sugerir el orden en que deben llevarse a cabo. La figura 13 muestra las etapas que esta metodología conlleva.

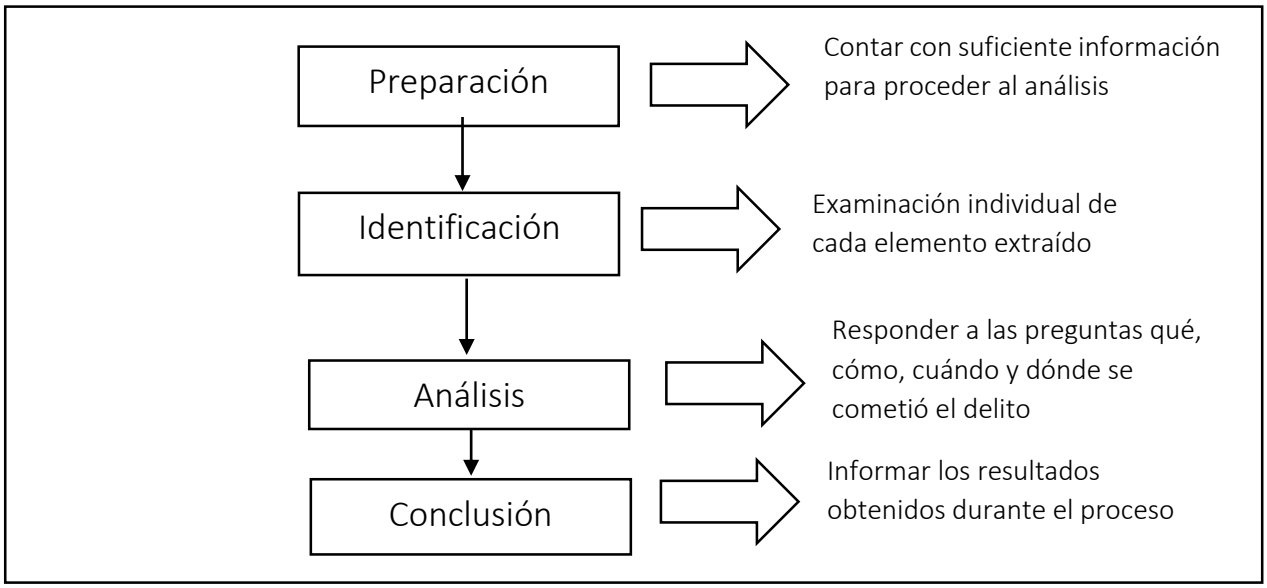


Figura 13: Metodología del departamento de Justicia USA
Fuente: Departamento de Justicia de los Estados Unidos (NIJ, 2004).

Guía Integral de Empleo de la Informática Foense en el Proceso Penal de Argentina

Lerena, Podestá & Constanzo, presentan "La Guía Integral de Empleo de la Informática Forense en el Proceso Penal en Argentina" aprobada en 2016 para orientar a profesionales de la informática forense y organismos judiciales en el proceso de obtener una evidencia digital válida (Lerena, Podestá, & Constanzo, 2016).

Esta guía se presenta dividida en seis fases, con lo cual se presentan los aspectos básicos a considerar en las labores relacionadas a la informática forense. La figura 14 muestra estas fases.

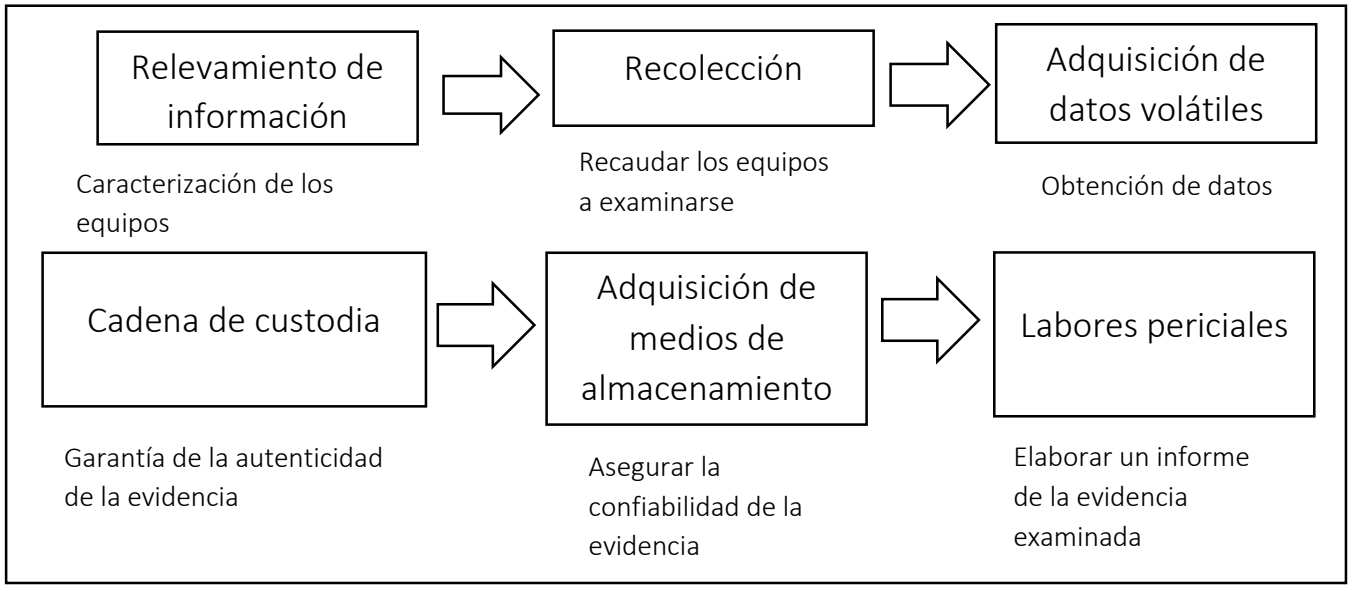


Figura 14: Etapas de la Metodología Argentina
Fuente: Guía Integral de empleo de la Informática Forense en el proceso penal en Argentina

A través de una investigación de campo tanto en la Fiscalía General como en la Policía Judicial se verificó las técnicas y protocolos usados para la investigación de los delitos cibernéticos se realizan siguiendo lo establecido en el "Manual de Manejo de Evidencias Digitales y Entornos Informáticos de la Fiscalía General del Ecuador" explicado anteriormente y los procedimientos dictados en el COIP.

Además, de la investigación que hace la Policía Judicial, el Consejo de la Judicatura utiliza como prueba las experticias de peritos particulares, calificados por el Consejo de la Judicatura, quienes son responsables, según la regulación 040-2014 emitida por el Consejo de la Judicatura del Ecuador denominada "Reglamento del Sistema Pericial Integral de la Función Judicial", en el capítulo IV, de:

Obligaciones generales:

- Realizar su trabajo con objetividad, imparcialidad, responsabilidad, oportunidad, puntualidad, rectitud, corrección y honestidad.
- Cumplir con la designación dispuesta por la autoridad judicial competente, la presentación del informe verbal y/o escrito, la presentación de aclaraciones, ampliaciones u observaciones al informe, la defensa y/o exposición del informe en audiencias orales, de prueba o de juicio; así como cualquier otra actividad necesaria dispuesta por autoridad judicial competente.

Obligaciones específicas:

- Cumplir la orden de la autoridad judicial una vez que han sido designados.
- Presentar el informe correspondiente oportunamente, en la forma, plazos y términos previstos por la normativa o por la autoridad judicial correspondiente.
- Subir los informes periciales al Sistema Informático Pericial, en archivo tipo PDF.
- Explicar y defender el informe presentado y sus conclusiones, en las audiencias orales, de prueba, o de juicio para las cuales fuere notificado legalmente, si la ley así lo prevé
- Entregar copia certificada de la factura de honorarios emitida por su persona, por el trabajo pericial realizado.
- Aprobar las capacitaciones establecidas por el Consejo de la Judicatura.

Se puede afirmar que la actividad de los Peritos Informáticos es parte del Sistema Judicial que a su vez tiene incidencia de otros actores como se resume en la siguiente gráfica:

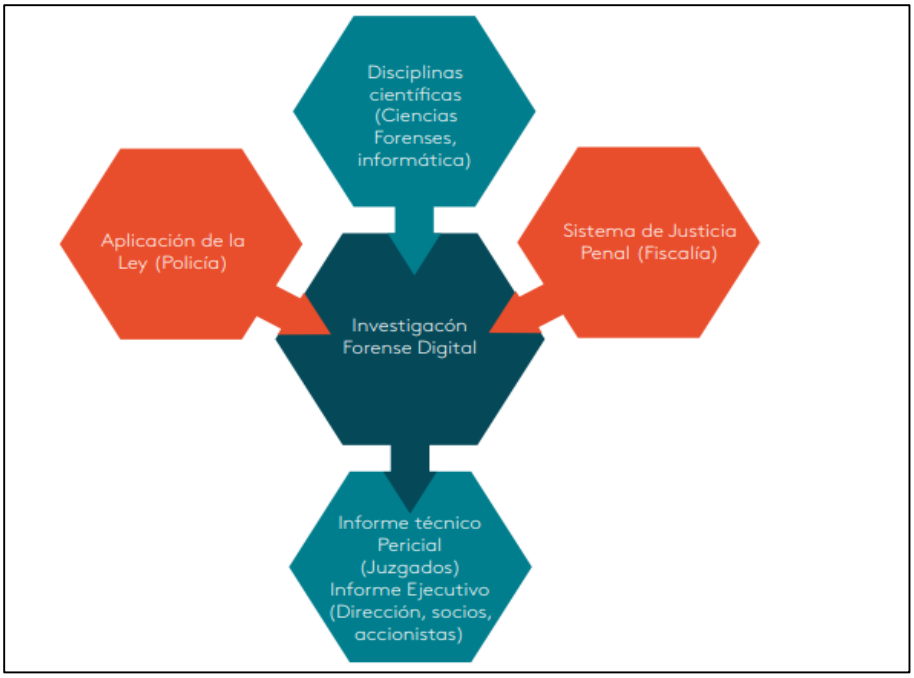


Figura 15: Factores que inciden en la investigación digital forense
Fuente: Kennedy, 2008

En el capítulo siguiente se presentará un estudio de campo donde se analizará el que hacer de los Peritos calificados por el Consejo de la Judicatura en el apoyo al juzgamiento de delitos, verificándose el cumplimiento o no de las normas y regulaciones que exige su actividad y tratando además de identificar que se cumplen estas etapas en la elaboración de sus informes. También se pretende a través del análisis a estos informes periciales confirmar los delitos comunes que requieren de pericias informáticas.

No todos los tipos de investigación que hacen los Peritos deben atender de forma estricta cada uno de los pasos de la investigación forense, pero siempre que los elementos sean aportados y analizados como prueba dentro de un proceso judicial deberán cumplir con todos y cada uno de los pasos previstos, tanto en la cadena de custodia como en el ciclo de la investigación forense, el cumplimiento o no de esos pasos verificará en el estudio de campo del capítulo 5.

Herramientas Tecnológicas Forenses

Para ayudar a los investigadores y Peritos, la industria de TI ha desarrollado algunas herramientas que ayudan a cuidar la evidencia digital y a el análisis de estas en el afán de encontrar a los responsables del cometimiento de un delito para su juzgamiento. A seguir se describen algunas de estas herramientas que se considera son las de mayor utilidad y reconocidas por los organismos de investigación de los diversos países.

TABLEU Bloqueador de escritura

El brigde forense Tableu eSATA ofrece más opciones de conexión nativa al equipo host y al dispositivo de almacenamiento a analizar, convirtiéndose en un útil bloqueador de escritura. Gracias a su kit de herramientas forenses, se puede disponer de un puente forense sólido y fiable con cuatro conexiones diferentes de la interfaz de host (eSATA, FireWire 800, FireWire 400 y USB) y de dos conexiones para dispositivos (SATA e IDE). La interfaz eSATA permitirá que los profesionales forenses adquieran imágenes de las unidades objeto de análisis SATA e IDE a una velocidad superior a FireWire 800. E incluso en algunos modelos puede hacer duplicados de discos de manera rápida.

En Case Forensic Toolkit

Es una plataforma de análisis forense digital desarrollado por Guidance Software que ofrece sus propias capacitaciones y certificaciones de la herramienta.

EnCase está diseñado para la seguridad cibernética, el uso del descubrimiento electrónico y el análisis forense. Permite recuperar datos y se utiliza en sistemas judiciales diferentes en todo el mundo. Se compone de herramientas utilizadas en diversas áreas del proceso forense digital, como el análisis, la adquisición y la generación de informes. Además, los usuarios cuentan con la versión portable, que les permite recopilar y recopilar información mientras se encuentran en la investigación de campo. EnCase Portable es una solución de adquisición de datos en una unidad USB. Busca en una computadora potencial y copia automáticamente datos que incluyen imágenes, historial de Internet, artefactos, documentos, incluso todo el disco duro y otras evidencias digitales (Fonrensic, 2019).

Características importantes:

- EnCase Forensic ofrece las capacidades de programación EnScript®. EnScript, un lenguaje de programación orientada a objetos y similar a Java o C++, les permite a los usuarios crear programas personalizados que los ayuden a automatizar las tareas de investigación que demandan mucho tiempo.
- CRC: imagen verificada por comprobación de redundancia cíclica (CRC) y MD5.
- Analizador de registro de eventos de Windows.
- Visualización nativa para 400 formatos de archivo.
- Búsqueda binaria: busca datos binarios sin procesar.
- Generación de informes: informes automáticos.

Ventajas:

- Especialmente útil cuando se reconstruyen RAIDs u obtienen acceso a discos duros cifrados.
- Permite encontrar evidencias para sumar cargos en una misma investigación.

- Permite crear una extensa base de datos vinculada (Crimen organizado).
- Captura, analiza y genera informes sobre evidencia digital.
- Permite recuperar evidencias digitales que habiten en archivos eliminados, discos reformateados, correo electrónico.

Desventajas:

- No soporta Outlook 2003 PST/OST.
- No genera informes robustos.
- La indexación necesita bastante trabajo para su correcta función.

IEF

Internet Evidence Finder MAGNET IEF es usado por millones de profesionales forenses alrededor del mundo con el fin de buscar, analizar y reportar la evidencia digital desde los computadores, Smartphones y Tablets.

Las potentes herramientas de análisis de IEF Report Viewer están diseñadas para permitir un análisis eficiente de grandes volúmenes de datos, lo que permite una rápida identificación de la evidencia más importante para una investigación (Robles, 2015).

Características importantes:

- Tiene compatibilidad con un amplio rango de imágenes. La opción de imágenes de IEF soporta los siguientes formatos de imagen: Imágenes de EnCase (.E01, .Ex01, .L01, .Lx01), imágenes de Forensic Toolkit (FTK) .AD1, Imágenes de máquina virtual (.vdi, .vhd, .vmdk, .xva), imágenes DMG, y formatos de archivo (.tar, .gz, .cpio, .zip, .z01).
- IEF agregó soporte para el montaje y análisis instantáneo de volumen de unidades e imágenes.
- IEF soporta Android, iOS, Windows.
- IEF tiene disponibles niveles de búsqueda, esto son: Full, Rápido Sectorizado, y personalizado.

Ventajas:

- Configurar IEF para procesar la carpeta del usuario en lugar de todo el disco duro puede potencialmente ahorrar horas de análisis innecesarios.
- El usuario puede configurar artefactos identificables, esto no solo permite un procesamiento más eficiente, sino que también permite al usuario realizar una revisión más específica y completa.
- IEF tiene gran facilidad para operar y navegar. Es decir, no es que es más fácil si no más inteligente que las otras aplicaciones forenses.
- Tan pronto como comienza el procesamiento, el usuario puede comenzar a revisar los datos procesados

Desventajas

- Magnet Forensics no ofrece ningún dispositivo del campo ni máquinas independientes.
- IEF tampoco ofrece ninguna ventaja relacionada con el cifrado o los teléfonos bloqueados, esta debilidad hace que IEF solo sea utilizable después de que el teléfono esté desbloqueado o sin cifrar

FTK

FTK es una plataforma de investigaciones digitales aprobada por tribunales, que se diseñó para ser veloz, analítica y contar con escalabilidad de clase empresarial. Conocida por su interfaz intuitiva, el análisis de correo electrónico, las vistas personalizadas de datos y su estabilidad, FTK establece el marco para una expansión, por lo que su solución de informática forense puede crecer de acuerdo con las necesidades del usuario (Snyder, 2018).

Características importantes:

- FTK funciona con bases de datos, por lo que no pierde el trabajo avanzado cuando la computadora tiene un crash o deja de responder.
- Procesamiento sin igual: procesa datos inmediatamente, por lo usted no pierde tiempo al esperar que se ejecuten las búsquedas durante la fase de análisis.
- Reportes robustos: genera reportes detallados en formatos originales, HTML, PDF, XML, RTF, entre otros.

Ventajas:

- Admite opciones y técnicas de búsqueda avanzadas, como la derivación.
- Interfaz de usuario GUI simple.
- Descifrado EFS.
- Creación del diccionario de contraseñas.

Desventajas:

- No es multitareas.
- Sin soporte de scripting.
- Límite de 2 millones de archivos.
- HFS (Mac) No es compatible

Nuix Investigator

Es una plataforma que permite recopilar, procesar, buscar y analizar rápidamente Terabytes de datos generados por humanos, llegando a los almacenes de datos más complejos de acceder. Es decir, Nuix nos ofrece una forma de hacer investigaciones inteligentes (NUIX, 2019).

Características importantes:

- Recopila datos de dispositivos propios, móviles, correos electrónicos, repositorios corporativos, la nube, redes sociales y unidades de red en un mismo caso para búsquedas y revisiones dinámicas.
- Nuix analiza enlaces sofisticadamente con el fin de visualizar que está mirando el usuario, donde está, con quien habla y que está haciendo.
- Elimina duplicados, genera diagramas de relaciones y verifica qué información se puede obtener de los datos.

Ventajas:

- Permite profundizar rápidamente en el qué, quién, cuándo y dónde de la evidencia del caso a través de gráficos e informes.
- Permite exportar los datos obtenidos de las búsquedas para operar con ellos.
- Se pueden encadenar una serie de actividades y ejecutarlas a la vez.
- Se puede realizar un análisis visual de forma interactiva e intuitiva de todos los datos del caso, de modo que, se pueden identificar tendencias, líneas de tiempo e información relevante en segundos.

Desventajas

- No tiene disponible buscador de Keywords.
- Necesita ser manipulado por abogados con buenas habilidades en TI, o experto en TI con conocimiento legal.
- Pocos ciclos de producción.

SANS Investigative Forensics Toolkit - SIFT

SIFT es una herramienta forense diseñada para realizar detallados exámenes forenses digitales y permitiendo usar una variedad de configuraciones para estos. SIFT demuestra que las capacidades avanzadas de respuesta a incidentes y las técnicas forenses digitales de inmersión profunda pueden lograrse mediante el uso de herramientas de código abierto de vanguardia que están disponibles de forma gratuita y se actualizan con frecuencia (Dynek, 2018).

Características importantes:

- Últimas herramientas y técnicas forenses.
- Compatibilidad cruzada entre Linux y Windows.
- Opción para instalar un sistema independiente a través del instalador SIFT-CLI
- Base Ubuntu LTS 16.04.
- Sistema base de 64 bits.
- Mejor utilización de la memoria.

Ventajas:

- Es una herramienta Open Source.
- Tiene una gran cantidad de scripts en Python incluidos.
- Tiene una herramienta de línea de tiempo.
- Tiene herramientas de análisis de memoria como Rekall.

Desventajas:

- SIFT puede rivalizar con los kits de herramientas forenses digitales comerciales con respecto a la funcionalidad, pero su GUI y la documentación del usuario son escasas.
- SIFT se recomienda para expertos forenses digitales certificados.
- Su índice de uso es relativamente bajo.

Una vez que se ha revisado las herramientas más destacadas para el manejo de evidencia digital, es necesario revisar los procesos de análisis y recopilación de evidencias que actualmente existen y permiten responder preguntas de dónde, cuándo, cómo y qué fue lo sucedido.

Guías de Investigación

RFC 3227 Directrices para la recolección de evidencias y su almacenamiento

Los RFC (Request For Comments) son documentos que recogen propuestas de expertos en una materia concreta, con el propósito de establecer ciertas pautas para la ejecución de un proceso, la creación de estándares o la implantación de algún protocolo (Proaño, 2012).

El RFC 3227 es un documento que recoge las directrices para la recopilación de evidencias y su almacenamiento, y puede llegar a servir como estándar de facto para la recopilación de información en incidentes de seguridad (Martínez, 2014).

Según los documentos RFC, los principios que deben seguirse para la recolección de evidencias son:

- Capturar una imagen del sistema lo más precisa posible.
- Minimizar los cambios en la información que se está recolectando y eliminar los agentes externos que puedan hacerlo.
- Elegir primero recolección y después análisis.
- Recoger la información según el orden de volatilidad (de mayor a menor).
- Tener en cuenta que por cada dispositivo la recogida de información puede realizarse de distinta manera.

Para preservar la integridad de la información, estas acciones deben evitarse:

- No apagar el computador hasta obtener toda la información.
- No confiar en la información proporcionada por los programas del computador.
- No ejecutar programas que modifiquen la fecha y hora de acceso de los ficheros del sistema.

Procedimiento de recolección

El proceso de recolección de información según RFC3227 debe ser lo más detallado posible, evitando ambigüedades y minimizando la toma de decisiones. El método de recolección debe ser transparente y reproducible. Los pasos por realizarse son:

- Listar los sistemas están involucrados y de cuáles de ellos se deben tomar evidencias.
- Establecer qué es relevante.
- Fijar el orden de volatilidad para cada sistema.
- Obtener la información de acuerdo con el orden establecido.
- Comprobar el grado de sincronización del reloj del sistema.
- Documentar cada paso.
- Tomar notas sobre qué gente estaba allí, qué estaban haciendo, qué observaron y cómo reaccionaron.

Procedimiento de almacenamiento

- Cadena de custodia: detallar como se descubrió, recolecto y manejo la evidencia. Indicar quién ha custodiado la evidencia y por cuanto tiempo se ha realizado.
- El almacenamiento de la evidencia debe realizarse en dispositivos que sean seguros e identifiquen intentos de acceso no autorizado.

Herramientas

Esta metodología propone que las herramientas a ser seleccionadas para el proceso de recolección deben cumplir con las siguientes características:

- Se deben utilizar herramientas ajenas al sistema.
- Se debe utilizar herramientas que alteren lo menos posible el escenario, evitando el uso de herramientas de interfaz gráfico y aquellas cuyo uso de memoria sea grande.
- Los programas que se vayan a utilizar para recolectar las evidencias deben estar ubicados en un dispositivo de sólo lectura (CDROM, USB, etc.).
- El kit de análisis debe incluir los siguientes tipos de herramientas:
    - Programas para listar y examinar procesos.
    - Programas para examinar el estado del sistema.
    - Programas para realizar copias bit a bit.

IOCE

La Organización Internacional de Evidencia Computacional (IOCE) publicó una guía denominada “Guía para las mejores prácticas en el examen forense de tecnología digital”. Esta guía proporciona estándares, principios de calidad y aproximaciones para un correcto manejo de la evidencia digital. La guía está estructurada de la siguiente manera (Zuccardi & Gutiérrez, 2006):

- Garantía de calidad (enunciados generales de roles, requisitos y pruebas de aptitud del personal, documentación, herramientas y validación de estas y espacio de trabajo).
- Determinación de los requisitos de examen del caso.
- Principios generales que se aplican a la recuperación de la evidencia digital (recomendaciones generales, documentación y responsabilidad).
- Prácticas aplicables al examen de la evidencia digital.
- Localización y recuperación de la evidencia digital en la escena:
    - Precauciones, búsqueda en la escena, recolección de la evidencia y
    - Empaquetado, etiquetando y documentación.
- Priorización de la evidencia.
- Examinar la evidencia: protocolos de análisis y expedientes de caso.
- Evaluación e interpretación de la evidencia.
- Presentación de resultados (informe escrito).
- Revisión del archivo del caso: Revisión técnica y revisión administrativa.
- Presentación oral de la evidencia.
- Procedimientos de seguridad y quejas.

DoJ1 y DoJ2

La Guía DoJ1 está basada en la recolección e identificación de evidencia, fue creada por el Departamento de Justicia de los EE. UU y también se denomina a esta guía como "Investigación En La Escena Del Crimen Electrónico" o en inglés: "Electronic Crime Scene Investigation: A Guide for First Responders" Esta guía tiene la siguiente estructura (Zuccardi & Gutiérrez, 2006):

- Dispositivos electrónicos (dispositivos habituales y su posible evidencia).
- Herramientas para investigar y equipo.
- Asegurar y evaluar la escena.
- Documentar la escena.
- Recolección de evidencia.
- Empaque, transporte y almacenamiento de la evidencia.
- Examen forense y clasificación de delitos.
- Anexos (glosario, listas de recursos legales, listas de recursos técnicos y listas de recursos de entrenamiento)

Varios países han optado por implementar sus propias guías para el manejo de evidencia digital. Por ejemplo, En Hong Kong se creó por medio de la Sociedad de Seguridad Informática y Forense una guía de mejores prácticas para la computación forense. En el Reino Unido se creó la "Guía De Buenas Prácticas Para Evidencia Basada En Computadores" por la Asociación de Jefes de Policía con el fin de ser usado a nivel interno de la organización. En Australia, la asociación de estándares australianos publicó la "Guía Para El Manejo De Evidencia En IT" que no está disponible para su libre distribución.

Certificaciones profesionales:

The Certified Forensic Computer Examiner (CFCE)

Esta certificación permite demostrar las competencias de un profesional en computación forense. Estas capacidades se evalúan utilizando el sistema operativo Windows. The International Association of Computer Investigative Specialists (IACIS) formada en el año de 1990 es la entidad encargada de capacitar y emitir los certificados del CFCE. Es una de las certificaciones sin uso de herramientas más reconocidas en informática forense para el personal policial actual.

Certified Fraud Examiners (CFE)

Este certificado es otorgado por la "Association of Certified Fraud Examiners" (ACFE). Las capacitaciones para obtener este certificado involucran conocimiento de transacciones financieras complejas, comprensión de los métodos forenses, las leyes, resolución de las denuncias de fraude. Una persona que posee el CFE tiene competencias para comprender como y porque se produjo el fraude (ACFE, 2019).

Para recapitular, es importante que se tome conciencia de las buenas prácticas a seguir cuando se debe tomar la evidencia digital, dado que esta nos permite usar la información adquirida en un juicio. En caso de que la evidencia digital llegue a ser manipulada, esta se considera inservible. Es por esta razón que es de suma importancia que los informáticos dedicados a su extracción dominen una o varias metodologías forenses para minimizar errores o perdidas en el proceso legal.

CAPÍTULO 5: Estudio de Campo, Análisis de las Pericias Técnicas en Delitos Juzgados en el Consejo de la Judicatura

Con el objeto de identificar los delitos en que se usan TICs, identificar las técnicas y metodologías que se aplican a las pericias técnicas, conocer las herramientas utilizadas tanto por los infractores como por los investigadores, saber las medidas de protección que emplean los usuarios de telefonía móvil, Internet y redes sociales; entre otros indicadores. Se procedió a realizar un trabajo de campo, para ello con el apoyo del Consejo de la Judicatura se obtuvo una muestra de 103 informes periciales empleados como pruebas en el juzgamiento de delitos cibernéticos. Y son los que se presentan a seguir y de los cuales se tratará de obtener los indicadores para el correspondiente análisis.

Investigación de campo

En este capítulo se procede a recolectar los datos provenientes del Consejo de la Judicatura y verificar qué se encuentra disponible y qué no. La organización no proporciona o estandariza las herramientas que deben ser usadas por los Peritos del área. Es decir, Pichincha se encuentra con un escenario donde cada profesional encargado de realizar una pericia debe hacerlo con los recursos que tenga disponible. Se cuenta con un total de 103 informes, dentro de las solicitudes de pericias se tiene:

Número de juicio	14304-2018-00313
Tema	Determinar origen de mensaje de una cuenta de Facebook y corroborar existencia de publicación.
Metodología aplicada	Informe basado en los principios establecidos en la norma ISO /IEC 27037:2012, que se establece como un guía de buenas prácticas para la identificación, recopilación y preservación de evidencias digitales, que permita un posterior análisis y documentación de resultados. Fases 1. Identificación de evidencia. - facilitada por la parte actora. 2. Recopilación de evidencia (Comentario y Perfil en la Red Social) Al no constar otro dato (identificador y/o URL (Localizador Uniforme de Recursos)) acerca del perfil de Facebook correspondiente a la cuenta de usuario, no se puede determinar que la cuenta este relacionada con el perfil de Facebook correspondiente. 3. Preservación de la evidencia.

Herramientas utilizadas en la pericia	- Herramienta de análisis de imagen Fotoforense.com

Número de juicio	17811-2016-00262
Tema	- Enlistar kits de grabación de una unidad judicial - Enlistar las audiencias que se grabaron con dichos dispositivos
Metodología aplicada	No se aplica, se verificó que cada Módulo de Grabación de Audiencias, cuente con una identificación etiquetado propio de la UNIDAD JUDICIAL por inventario de bienes, y los números de series propias del fabricante.
Herramientas utilizadas en la pericia	Sistema Cicero Access Data Software para captura de Imagen forense

Número de juicio	07257-2018-00171
Tema	Realizar pericia técnica de una cuenta de red social de Facebook.
Metodología aplicada	Procedimiento descriptivo: - En primer lugar, se procedió a fijar fotográficamente el material recibido para peritación (estuche o sobre contenedor). - Se retiran las seguridades con las que contaba el DVD-R sacándolo del estuche que lo contenía. - Se procedió a verificar visualmente la integridad física del DVD-R, no encontrando alteraciones en su estructura. - Mediante el uso del programa Explorador de Windows se procedió a realizar la verificación de información almacenada en el DVD-R encontrando un video de nombre 20180327_083150. - Se procede a realizar la explotación de la cuenta de la red social de Facebook del denunciado Orlin Israel Castro Vásquez. - Se procede a verificar las publicaciones de fecha. - Se procede a realizar las capturas de pantalla de la información de la cuenta y de la publicación de la cual se solicita la pericia. - Se procede a realizar la grabación de un video en formato MP4 del perfil de Facebook de la cuenta, el mismo que se graba en un CD-R y el cual tiene una duración de 7 minutos y 52 segundos y un tamaño de 14,8 MB para su respectivo análisis y verificación.

Herramientas utilizadas en la pericia	No aplicadas

Número de juicio	11333-2015-05689
Tema	Recuperar e identificar los correos electrónicos que fueron enviados los días del 3 al 11 de noviembre de 2009, a la cuenta de jo**ar@hotmail.com
Metodología aplicada	Metodología descriptiva del uso del software.
Herramientas utilizadas en la pericia	- Software para calcular un valor hash del archivo contenedor de los mails - Who.is identificador de dominios

Número de juicio	01618-2017-00148
Tema	Extracción de información de un medio digital que se adjuntó.
Metodología aplicada	La metodología utilizada contiene las siguientes etapas: 1. Búsqueda de datos relevantes para el análisis. 2. Identificación y categorización de los datos encontrados. 3. Comprobar integridad de los datos. 4. Identificar importancia de los datos para la investigación y 5. Realizar conclusiones sobre los datos obtenidos
Herramientas utilizadas en la pericia	- Software para el cálculo del Hash MD5 - Software para conocer los tipos de archivo, la fecha y hora, así como la data correspondiente a la fecha de última modificación de la información administrativa del archivo.

Name	Last Accessed	MD5	SHA1	Entry Modified
01618-2017-00148				
Session-1		3e6f4ed0d6d7e2026292922339205e5b	d066e184381b453ea56ab4086a6e1e6a74b52a87	
09 ene 2018 (UDF)				
UDF Volume Set		b2bff948f13a10aec7519101b6b15ba9	7c25f00b51e2f0cc93af905eedb1697002fbb33d	
video.mp4	**01/09/18 10:39:24 AM**	**743d31902caf0df162edeff8c8627fd8**	**824264e299816bc22040110e189008a31ea31c50**	**01/03/18 07:58:36 PM**
IMG-20180103-WA0007.jpg	**01/09/18 10:41:41 AM**	**05209438bf9fde3a91b7eedb17ab21c3**	**3505affac289a715ba6e2d9df59d62bdb8d79b35**	**01/03/18 08:01:25 PM**

Fuente: Informe Pericial del Consejo de la Judicatura con ID: 01618-2017-00148

Número de juicio	01283-2018-01072
Tema	Reconocimiento y transcripción de un audio y video.
Metodología aplicada	La metodología utilizada contiene las siguientes etapas: 1. Generación de una imagen forense del CD con número de serie: TBZ705154624E17 2. Extracción e identificación de los archivos presentes en la unidad de almacenamiento. 3. Creación de imágenes de los archivos de video existentes en la unidad de almacenamiento, 4. Transcripción de audio de los archivos de la unidad de almacenamiento. 5. Correlacionar imágenes creadas y transcripción realizada. 6. Realizar conclusiones sobre los datos obtenidos.
Herramientas utilizadas en la pericia	- Encase: software para generar imagen forense del CD - Exiftool

Número de juicio	01283-2018-01297
Tema	Pericia de la publicación en la red social “Facebook” del perfil “W** Fe**do V**ez So**s” en el grupo “Comunidad Cuenca”, con el fin de determinar el perfil del cual se realizó la publicación
Metodología aplicada	Metodología aplicada: • Identificación: identificar las evidencias

	• Recolección: determinar fuentes de información, adquisición o extracción mediante técnicas y herramientas • Análisis: examinar la información obtenida • Resultados: elaboración y entrega de informe pericial Técnicas aplicadas: • Reconocimiento o footprinting • Procedimiento ELA (análisis de errores de nivel) • Técnica inversa de imágenes
Herramientas utilizadas en la pericia	• FotoForensics • Google Images • Herramienta de desarrollo de la página web • Maltego

Número de juicio	01283-2018-02993G
Tema	el resultado de la experticia realizada a la página web "https://www.facebook.com/search/top/?q=adivinen%20quien%20es%20este%20angelito", correspondiente a una publicación realizada en la página de la red social "Facebook" donde se encuentran imágenes que incluyen al señor C***s A****s R****o A****o. Donde se determinará: • Origen de la publicación • Número de veces que la publicación es compartida. • Número de reacciones emitidas o generadas en la publicación.
Metodología aplicada	• Revisión de código fuente HTML. • Se identifica el nombre de usuario con su respectivo ID de la cuenta de Facebook. • Verificar el URL de origen. • Analizar comentarios e imágenes.
Herramientas utilizadas en la pericia	No se utilizan.

Número de juicio	03332-2017-00565
Tema	Extraer el video que consta en el teléfono celular Samsung adjunto a la demanda con nombre de archivo 20170719_210731 y

	adjuntar al proceso en algún dispositivo de almacenamiento magnético u óptico de fácil reproducción
Metodología aplicada	1. Adquisición de datos desde el dispositivo móvil 2. Generación de Hash del archivo 3. Análisis de Meta Data 4. Conclusiones 5. Inclusión de documentos de respaldo o anexos
Herramientas utilizadas en la pericia	• MD5 & SHA Checksum Utility 2.1 • Herramienta ADB (permite acceder a los datos e información del dispositivo desde el equipo del examinador y ejecutar algunos comandos que van a permitir la extracción de los datos) • Herramienta Exiftool: Extracción de la información de la meta data del archivo

Número de juicio	01283-2018-00098
Tema	El reconocimiento y transcripción del contenido de los discos compactos de audio y video presentados por la compareciente
Metodología aplicada	Descriptiva del resultado obtenido de la herramienta.
Herramientas utilizadas en la pericia	Easytranscript: Utilizada para visualizar y escuchar los CD y realizar la respectiva transcripción.

Número de juicio	17371-2017-05550
Tema	Realizar el análisis del archivo que se encuentra en el cd, con la finalidad de realizar la verificación de la de información.
Metodología aplicada	- Alcance - Descripción del objetivo de análisis - Prueba pericial - Conclusiones

Herramientas utilizadas en la pericia	- Nero StartSmart: permite obtener copias de los CD

Número de juicio	18371-2018-00154
Tema	Revisar los recorridos de las unidades en el GPS, coincidencias de ubicación y lugares donde permanecieron estacionados durante el día 12 de abril de 2018.
Metodología aplicada	lineamientos de la RFC 3227 (Request For Comments o Directrices para la recopilación de evidencias y su almacenamiento) y el instructivo del Reglamento General de Peritos del Ecuador
Herramientas utilizadas en la pericia	- KunanSoft: plataforma de rastreo - AccessData FTK Imager 3.1 para - garantizar la integridad de la evidencia digital

Número de juicio	03203-2018-00254
Tema	Análisis del contenido de los dos discos que contienen conversaciones incriminadoras y su originalidad.
Metodología aplicada	Descriptiva basada en cuatro fases: 1. Antecedentes 2. Planteamiento del problema 3. Verificación 4. Conclusiones
Herramientas utilizadas en la pericia	ADOBE AUDITION CC 2018 Se realiza la transcripción de los audios manualmente

Número de juicio	17308-2011-1444
Tema	Verificar: • La existencia de un servidor IBM Power System 520 modelo 8203-E4A, número de serie 0662b06

	• Determinar si el sistema denominado Galileo se encuentra operativo en el servidor peritado • Determinar si el sistema indicado, cuenta adicionalmente con el desarrollo informático complementario, especial para la empresa TRAMACOEXPRESS • Las bondades y usos que puede brindar el sistema analizado • Fecha de creación y cierre del mismo (desde cuándo se encuentra listo para operar o ser utilizado)
Metodología aplicada	Ninguna utilizada. Descriptiva de la revisión física realizada. Revisión de los documentos enviados por IBM, los cuales constan con la marca, modelo y número de serie del servidor.
Herramientas utilizadas en la pericia	Ninguna

Número de juicio	11282-2017-01313
Tema	Identificar y extraer videos. Siguiendo los principios: La evidencia debe ser adquirida del modo menos intrusivo posible. Análisis de metadatos. (propiedades internas de un archivo) El valor hash (valida la integridad de la información MD5, SHA1)
Metodología aplicada	Descriptiva
Herramientas utilizadas en la pericia	AppleQuickTime para la creación de imágenes y videos (utilizado por los infractores)

Número de juicio	11282-2017-00739
Tema	Apertura, extracción de la información y trascripción del contenido del audio de un CD y un flash memory.
Metodología aplicada	- Cargar el CD de audio en la unidad DVD RW de un computador.

	- Cargar el archivo de audio en el software profesional ADOBE AUDITION, verificar propiedades del archivo, que la trama de audio sea consistente, regular y que no posea alteraciones. - Verificar la calidad de audio, de existir ruido ambiental, realizar suavizado del mismo. - Identificar a los locutores que intervienen en la grabación y asignar un código o nombre personalizado. - Transcribir la conversación identificando tiempo, locutor y contenido de la conversación.
Herramientas utilizadas en la pericia	- Adobe Audition - Express Scribe Pro para la transcripción del audio.

Número de juicio	15301-2017-01000
Tema	Transcripciones de audios
Metodología aplicada	Ninguna
Herramientas utilizadas en la pericia	Ninguna

Número de juicio	11203201703613
Tema	Verificación de las llamadas telefónicas recibidas al teléfono de la señora Li**a J***z M**o con número 0986117208 por parte del número 0969673299.
Metodología aplicada	Verificar que el número del celular pertenezca al propietario análisis del registro de llamadas
Herramientas utilizadas en la pericia	Ninguna

Número de juicio	17294-2018-00101
Tema	Establecer perfil, usuario y cuenta, dueño de la cuenta de Facebook, Twitter y datos de conectividad de las URL.

Metodología aplicada	1. Recopilación de pruebas 2. Análisis técnico de las URL
Herramientas utilizadas en la pericia	Network Tools: determina la existencia del link

Número de juicio	17811-2016-00262
Tema	Extracción y materialización de 4 ejemplares de todos los documentos existentes en el mencionado sitio.
Metodología aplicada	- Extracción de las muestras del sitio de INDRA SISTEMAS de la siguiente URL: https://operaciones.indra.es/cliente/JC/JIC/default.aspx. - Indexación de documentos para elaborar un mapa de archivos. - Materialización de muestras por un total de 5 ejemplares. - Clasificación de documentos. - Anillado de documentos. - Entrega.
Herramientas utilizadas en la pericia	Ninguna

Número de juicio	06335-2016-00567
Tema	Realizar el evaluó de los equipos informáticos.
Metodología aplicada	1. Análisis y evaluación de equipos 2. Realizar el inventario
Herramientas utilizadas en la pericia	No utiliza

Número de juicio	07331-2015-00190
Tema	Determinar si en las imágenes se visualiza el predio materia de la Litis
Metodología aplicada	1. Referenciar las imágenes analizadas en la pericia 2. Detalles técnicos del archivo

	3. Comparativa con respecto al tiempo de la zona analizada.
Herramientas utilizadas en la pericia	Google Earth Pro Digitalglobe: Satelite

Número de juicio	05254-2017-00211
Tema	Realizar con claridad el peritaje en las redes sociales de Facebook e Instagram para establecerse que la publicación si existió.
Metodología aplicada	No utilizada
Herramientas utilizadas en la pericia	- Ingeniería social - Redes sociales Facebook e Instagram.

Número de juicio	07331-2018-00092
Tema	Determinar el Contenido de la Información dentro del Juicio de Despojo Violento.
Metodología aplicada	Metodología descriptiva, relacionado lo extraído del audio con las imágenes de los hechos.
Herramientas utilizadas en la pericia	- VLC Media Player, que es un reproductor multimedia, gratuito y multiplataforma. - Un Driver llamado VB-CABLE Virtual Audio Device que permite poder pasar el audio de un archivo de video hacia alguna otra aplicación que lo recepte como entrada para procesarlo - La aplicación en línea SpeechLogger que procesa la información del audio del computador y hace uso del Driver anteriormente manifestado. - Para determinar el contenido del audio de video a texto se utilizó la aplicación en línea SpeechLogger que es un reconocimiento de voz, esta aplicación utiliza la tecnología de Google.

Número de juicio	17811-2015-01595
Tema	- Verificar la existencia de los kits para salas de grabación de audiencias para salas fijas entregadas. - Enlistar los dispositivos entregados.

	- Verificar los números de serie de los dispositivos. - Enlistar las audiencias que se grabaron con dichos equipos. - Determinar el funcionamiento de los equipos. - Verificar si el sistema de grabación de audiencias Cicero fue borrado.
Metodología aplicada	- Las prácticas técnicas consistieron en: - Comunicación con personal de Unidad Judicial de familia, mujer y adolescencia solicitando permiso y facilidades para efectuar el peritaje informático. - Observación de las instalaciones - Revisión de la documentación - Inspección de los equipos entregados mediante actas entrega recepción - Levantamiento de información - Recolección de evidencia - Documentación fotográfica. - Probar el software para grabación de audiencias. - Verificar estado del Software CICERO
Herramientas utilizadas en la pericia	- Software Cicero - Sistema SAGA para realizar la grabación de audiencias.

Número de juicio	17811-2016-00268
Tema	- Verificar la existencia de los kits para salas de grabación de audiencias para salas fijas entregadas. - Enlistar los dispositivos entregados. - Verificar los números de serie de los dispositivos. - Enlistar las audiencias que se grabaron con dichos equipos. - Determinar el funcionamiento de los equipos.
Metodología aplicada	- Reunión con personal de la Dirección Nacional de TICS - Observación de las instalaciones - Revisión de la documentación - Inspección de los equipos entregados mediante de actas entrega y recepción - Levantamiento de información - Recolección de evidencia - Documentación fotográfica. - Ejecución
Herramientas utilizadas en la pericia	-Software Cicero

Número de juicio	01283-2016-03420
Tema	Extracción de la información de la cuenta de Facebook perteneciente a Daniel Alonso Lazo Zhagui y Olga Beatriz Zhagui Juncal, en donde constan los mensajes de texto en tono amenazante, enviados por parte del querellado
Metodología aplicada	- Descriptiva
Herramientas utilizadas en la pericia	Ninguna

Número de juicio	01331-2017-00189
Tema	Experticia de Ingeniera Informática o de Sistemas dentro del proceso de acción COBRO DE LETRA DE CAMBIO. Realizar un peritaje informático para que se revise el sistema computarizado que manejan de los pagos hechos a la accionante de intereses del préstamo. Se indique el monto total al que asciende dichos pagos y si el sistema utilizado es confiable imposible de manipular alterando fechas y/o cantidades de los diversos pagos realizados.
Metodología aplicada	- Experimental
Herramientas utilizadas en la pericia	- Servidor local - Microsoft Access 2010

Número de juicio	07307-2017-00308
Tema	Se revise el sistema Informático contable desde el año 2014 al año 2016, para obtener el detalle, numero, fechas, y montos de las facturas emitidas en favor del señor Homero Ferdinan Rojas Vera.
Metodología aplicada	Descriptiva. Descripción de las imágenes capturadas del sistema informático contable “Tisoft” de la empresa distribuidora.
Herramientas utilizadas en la pericia	Programa Tisoft

Número de juicio	09285-2014-2449
Tema	Todos los tuits existentes en la cuenta @**esa a partir del 10 de enero del año 2014 hasta el 31 de enero del 2014, con determinación del titular de dicha cuenta.
Metodología aplicada	- Autenticación en Twitter con la cuenta de usuario: Kas**oB. - Buscar la cuenta @**sa y obtener acceso a los tweets recientes publicados en la misma. - Determinar que el titular de la cuenta @*** de acuerdo con la información mostrada por Twitter. - Se procedió a cargar los tweets publicados por la cuenta @**esa durante el mes de enero del 2014. - Se efectuó además una auditoría de la cuenta @**esa para determinar el número de seguidores reales de dicha cuenta con ayuda de la utilidad TwitterAudit.
Herramientas utilizadas en la pericia	TwitterAudit.

Número de juicio	09284-2013-0175
Tema	Determinar si en el Sistema de Comercialización y Gestión de Medicina Prepagada de la empresa SALUD S.A. Sistema de Medicina Prepagada del Ecuador S.A. existen registros respecto a atenciones y reclamos del ciudadano Medina Acosta Jorge con número de cédula 0903517589.
Metodología aplicada	- Acceder al Sistema de Comercialización y Gestión de Medicina Prepagada. - Autenticarse en el sistema y acceder a los registros referentes al ciudadano. - Extraer información correspondiente. - Verificar registros en la base de datos PROGRESS.
Herramientas utilizadas en la pericia	- Sistema de Comercialización y Gestión de Medicina Prepagada de la empresa SALUDSA SISTEMA DE MEDICINA PREPAGADA DEL ECUADOR S.A. - Base de Datos PROGRESS

Número de juicio	07333-2015-0306

Tema	Realizar experticia a los correos electrónicos richarvj@hotmail.com y pgarrido62@gmail.com
Metodología aplicada	- Solicitar contraseña a los propietarios de las cuentas de correo - Verificar bandeja de entrada - Buscar en la bandeja de entrada correo con dominio "arcom.gob.ec" - Revisar bandeja de eliminados
Herramientas utilizadas en la pericia	Whois

Número de juicio	01371-2015-0138
Tema	- Determinar, descargar e imprimir todo el historial de la cadena de emails enviados desde los usuarios autorizados de la empresa TEDASA S.A - Acreditar la veracidad de los mismos, origen fechas y desmaterialización completa de los mismos.
Metodología aplicada	- Acceder al servidor de correo electrónico - Identificar las cuentas de correo, obrantes - Ordenar los correos electrónicos por la fecha, verificando que el correo más antiguo que consta como recibido en el buzón - Corroborar la veracidad de los mensajes comprobando que fueron enviados atreves del servidor de correo que la empresa Tedasa S.A - Extraer los mensajes de correo encontrados, procediendo a firmarlos digitalmente con un código HASH
Herramientas utilizadas en la pericia	Servidor de correo Zimbra2 en su versión 8.6.0, utilizado por la empresa.

Número de juicio	01371-2015-00351
Tema	Verificar el sistema de control de asistencia, esto es ingreso y salida del trabajo del demandante, durante el tiempo que mantuvo su relación laboral.
Metodología aplicada	Descriptiva: - Ir a las instalaciones de la empresa demandada.

	- Constatar que no existe un equipo de marcación de asistencia del personal, ni un software informático que realice dicho control del personal de la compañía.
Herramientas utilizadas en la pericia	Ninguna

Número de juicio	01371-2015-00435
Tema	Verificar el contenido de los correos electrónicos enviados a la cuenta de correo ynancyqv@hotmail.es, provenientes de los correos secretaria@cruzrojaazuay.org y jcgerencia@cruzrojaazuay.org.
Metodología aplicada	- Acceder a la cuenta de correo con credenciales facilitadas por el usuario - Extraer los correos pertinentes - - Para verificación y en cumplimiento de los regímenes de cadena de custodia dictados por el COIP se procedió a generar las firmas HASH1 a cada uno de los archivos digitales.
Herramientas utilizadas en la pericia	Ninguna especificada.

Número de juicio	09354-2014-0702
Tema	Análisis del Sistema Informático para el control y registro de marcaciones de la actora, durante todo el tiempo de relación laboral.
Metodología aplicada	- Entrevista al área de sistemas sobre el área técnica del aplicativo - Entrevista con el área de nóminas para revisar el funcionamiento del usuario por parte del aplicativo - Explicación del Registro de Entrada y Salida - Análisis de información de los datos extraídos de su periodo laboral.
Herramientas utilizadas en la pericia	Sistema denominado SCES002 que pertenece a la infraestructura AS/400, en la herramienta de programación RPG400 y base de datos DB@

Número de juicio	01371-2015-00538
Tema	Se solicita realizar una pericia sobre el sistema Medisys, que mantiene el Hospital Vicente Corral Moscoso, y constatar la existencia del usuario AMACHUCA Y FMATUTE.
Metodología aplicada	- Ingresar al sistema Medisys para la búsqueda de los datos objeto. - Buscar el usuario en el sistema. - Verificar dentro del sistema los movimientos realizados por este usuario consultando las Transacciones de bodega realizadas como son los egresos de medicinas.
Herramientas utilizadas en la pericia	Sistema Medisys (sistema interno de la empresa)

Número de juicio	01371-2015-00761
Tema	Realizar la Inspección al sistema y registro digital de asistencia y marcación de la trabajadora por el tiempo de la relación laboral, se constate y se establezca la asistencial al trabajo, así como las horas laboradas.
Metodología aplicada	La Base de Datos se encuentra en Informix y el lenguaje de programación en 4GL; La seguridad aplicada a la Base de Datos se realiza mediante replicas entre servidores; por lo que se determina que cumplen con la norma requerida. No existen procesos manuales de cambios sobre la base de datos; El registro de la asistencia del personal se lo realiza en base a la cedula que se digita al ingresar y salir de su lugar de trabajo;
Herramientas utilizadas en la pericia	Informix Lenguaje de programación 4GL

Número de juicio	01151-2013-1551
Tema	Establecer el recorrido o trazabilidad de mensajes en la red y conocer su destino final; a que direcciones electrónicas fueron enviados desde la dirección electrónica del demandado, tal como lo he pedido en mi demanda y en todo el proceso

Metodología aplicada	No procede con la pericia. Técnicamente imposible si no se dispone del acceso a las cuentas de quienes recibieron dichos mensajes
Herramientas utilizadas en la pericia	No utilizada.

Número de juicio	01801-2012-0392
Tema	- Identificar por beneficiario (lESS) dentro del módulo Tesorería de la Institución en: Gestión de Giros y Transferencias, Ítem Reportes, en relación de pagos y su estatus. - Determinar el detalle de la fecha de confirmación de pago, de los meses de marzo y diciembre de 2009, en lo referente al pago de las obligaciones de la Universidad de Cuenca a favor del Instituto Ecuatoriano de Seguridad Social. - Del análisis del sistema y documentación existente en el mismo, indicar si la Universidad de Cuenca, cumplió con sus obligaciones ante el Instituto Ecuatoriano de Seguridad Social.
Metodología aplicada	- Acceder al sistema del Ministerio de Finanzas SIGEF, utilizando el usuario m***oso - Verificar y descargar los aportes institucionales a favor del Instituto Ecuatoriano de Seguridad Social
Herramientas utilizadas en la pericia	Se utilizó el sistema utilizado por el Ministerio de Finanzas SIGEF para corroborar la información.

Número de juicio	11333-2014-2923
Tema	Realizar el avalúo de los bienes incautados detallados en el acta que obra de fojas 64, 65 y 66 del presente proceso, los mimos que se encuentran en custodia del Depositario Judicial.
Metodología aplicada	Descriptiva de la evidencia y exploratoria para dar con las personas involucradas en el audio
Herramientas utilizadas en la pericia	Ninguna en la transcripción del audio

Número de juicio	13331-2016-00160
Tema	Evaluar la infraestructura de la Radio base ubicada en el cantón Jipijapa, propiedad de la compañía Consorcio Ecuatoriano de Telecomunicaciones, S.A. CONECEL
Metodología aplicada	Descriptiva del trabajo de los elementos observados dentro de la radio base objeto de la inspección para poder inferir la información - Tablero de energía - Generador eléctrico - Equipos de radio frecuencia - Torre Monopolo - Antenas celulares
Herramientas utilizadas en la pericia	No utilizada

Número de juicio	17151-2017-00137
Tema	Realizar una pericia del equipo celular Iphone 7, que registra el número 0993966320, en la parte pertinente a la recepción de mensajes del sistema WhatsApp del número 0994235932 de Roberto Barrera, del sábado 04 de marzo de 2017, certificando el contenido y la autenticidad de la información digital de dicho equipo celular.
Metodología aplicada	Se verificó el número IMEI del celular marcando la opción *#06# Se busca el contacto requerido Mediante técnicas forenses se extrajo la información la cual se captura las imágenes que el software dio como resultado luego del análisis del equipo
Herramientas utilizadas en la pericia	Plataforma WhatsApp para la verificación de la información.

Número de juicio	17811-2015-01239
Tema	Evaluar el equipo AZBox evoXL, explicar funcionalidad de los elementos involucrados en un sistema de televisión satelital

Metodología aplicada	Descriptiva del funcionamiento de un sistema de televisión satelital, y cómo funciona la piratería al desencriptar la señal para su uso ilegal.
Herramientas utilizadas en la pericia	software NAGRA desarrollado por NAGRAVISION S.A. Análisis forense

Número de juicio	11333-2013-14637
Tema	Realizar el avalúo de los bienes embargados que se encuentran en custodia del señor depositario Judicial. Utilizar el sistema vigente de Remates Judiciales en línea para subir la información contenida en el presente informe respecto a los bienes embargados.
Metodología aplicada	Descriptiva referente a los bienes incautados
Herramientas utilizadas en la pericia	Ninguna

Número de juicio	17113-2014-3252
Tema	Transcripción de la entrevista realizada el día 7 de junio del 2006
Metodología aplicada	- Tomar como referencia el instructivo del informe pericial de audio, video y afines, publicado por la Fiscalía General del Ecuador. - Realizar la extracción del código HASH MD5 del archivo. - Se realiza la transcripción de la entrevista. - Se procede a materializar la entrevista.
Herramientas utilizadas en la pericia	Programas de ofimática Software HashMyFiles.

Número de juicio	07331-2017-00443
Tema	Explotación de todo el CD de las imágenes, sonidos, videos, voces e identificar a las personas que participan en este cd adjuntado por los actores.
Metodología aplicada	- Fijar fotográficamente el material recibido para peritación (estuche o sobre contenedor).

	- Se retiran las seguridades con las que contaba el CD-R sacándolo del estuche que lo contenía. - Fijar fotográficamente el CD-R (lado frontal y lado posterior). - Se procedió a verificar visualmente la integridad física del CD-R, no encontrando alteraciones en su estructura. - Se verifica visualmente indicios de escritura en la superficie fotosensible del CD-R no observando rastro alguno. - Mediante el uso del programa Explorador de Windows se procedió a realizar la verificación de información almacenada en el CD-R no encontrando información alguna localizada en el CD-R.
Herramientas utilizadas en la pericia	Navegador de Internet Explorer

Número de juicio	07307-2015-00354
Tema	Verificar si la cooperativa Santa Rosa Tiene DATA WAREHOUSE o repositorio de datos con variables sociodemográficas, de comportamiento de pagos de flujos de ingresos y gastos, etc.
Metodología aplicada	Exploratoria
Herramientas utilizadas en la pericia	INFORMIX Oracle Software Focus Credit Risk, SIGECOB y SASC pertenecientes a CAEFYC

Número de juicio	09359-2015-04009
Tema	Extracción de la información presentada como evidencia
Metodología aplicada	Se procede a evaluar y examinar los archivos del pen drive
Herramientas utilizadas en la pericia	Se utilizó las consultas del sistema operativo propio del equipo de cómputo. Digital Forensics Framework Para revisión de los videos se utilizó el Reproductor de Windows Media El programa Defraser.

Número de juicio	10333-2016-00560
Tema	Verificación de la conversación por la red social
Metodología aplicada	Descriptiva de la conversación visualizada en la red social.
Herramientas utilizadas en la pericia	Red social Facebook

Número de juicio	07281-2017-00009
Tema	Transcripción de todo el CD de las imágenes, sonidos, luces, voces, e identificar a las personas que participan en este video adjuntado por la demandada.
Metodología aplicada	- Fijar fotográficamente el material recibido para peritación. - Verificar visualmente la integridad física del CD-R con el programa "Reproductor de Windows Media" para la visualización de videos (Imagen y Sonido) - Verificar la calidad y contenido de la grabación del archivo de video que obra en el CD-R objeto de análisis. - Capturar las imágenes idóneas de la secuencia de imágenes de los archivos de video que obran en el CD-R objeto de análisis.
Herramientas utilizadas en la pericia	No utiliza, sin embargo, afirma que la evidencia no presenta alteraciones.

Número de juicio	13311-2015-00464
Tema	Realizar una pericia a un CD y un DVD-R marca Imation código MFP353RK1417364044 donde se solicita que se realice la correspondiente transcripción en forma textual de los elementos presentados CD Y DVD-R
Metodología aplicada	- Recopilación de la información - Verificación de contenido - Extracción de información desde la cuenta personal de correo electrónico del señor Marco Tulio Giler Mendoza - Análisis del Contenido de la Información transcripta
Herramientas utilizadas en la pericia	No utilizadas, la transcripción se realizó manualmente.

Número de juicio	13337-2016-01224
Tema	extracción de las conversaciones mantenidas con el señor FABIAN ALVARADO VALENCIA en mi cuenta de FACEBOOK andrs.giler@hotmail.com
Metodología aplicada	- Recopilación de información de la plataforma de Facebook - Recopilación y extracción de información del perfil de usuario de Carlos Andrés Giler Castillo - Información recopilada del perfil de usuario de Fabian Alvarado - Extracción de Información desde la aplicación WhatsApp configurada con el número 0983392558 instalada en el teléfono HUAWEI Ascend Y530. - Análisis de la información extraída del usuario
Herramientas utilizadas en la pericia	Plataformas de redes sociales para extraer información.

Número de juicio	3371-2015-00484
Tema	Realizar un peritaje a la bitácora de ingreso y salida del personal de la compañía MantaOro hotelera S.A.
Metodología aplicada	- Recopilación de información - Revisar las marcaciones de ingreso y salida en la bitácora del demandante - Verificar el ultimo registro
Herramientas utilizadas en la pericia	No utilizada por parte del Perito

Número de juicio	17230-2015-16900
Tema	Realizar una experticia informática consistente en la fijación, extracción, análisis y materialización de correos electrónicos con sus respectivos adjuntos, recibidos en el servidor de la empresa FIDUCIA S.A,
Metodología aplicada	- Especificar definiciones importantes para la pericia - Buscar y obtener los correos electrónicos del servidor de la organización - Fijación de los correos

	- Extraer y materializar los correos electrónicos y los adjuntos que existen en los correos electrónicos - Extraer y materializar los adjuntos que existen en los correos electrónicos. - Obtener las cabeceras de los correos electrónicos.
Herramientas utilizadas en la pericia	Servidor de correo para extracción de información Aplicación Outlook Web Access (OWA)

Número de juicio	17293-2017-00535
Tema	Extracción de información en el link de la Fiscalía General del Estado de la Noticia Crímenes No. 170501817050038
Metodología aplicada	- Ingreso en la página web de la Fiscalía General del Estado. - Búsqueda de la noticia con el código señalado. - Extracción de la información que se encuentra en la página web.
Herramientas utilizadas en la pericia	URL www.fiscalia.gob.ec (acceso a internet)

Número de juicio	01604-2014-0354
Tema	Revisar y verificar la existencia de documentos presentados en el proceso por parte del demandante en el sistema de gestión documental QUIPUX.
Metodología aplicada	- Ingreso al sistema solicitando contraseñas del administrador - Recolección de información mediante consultas al sistema. - Determina existencia de evidencia en el sistema - Adjuntar copia digital de evidencia
Herramientas utilizadas en la pericia	Sistema QUIPUX

Número de juicio	01802-2014-0205
Tema	Examinar los metadatos de los siguientes documentos según se describe en el proceso
Metodología aplicada	- Ingresar a ver metadatos del dispositivo - Realizar capturas de pantalla correspondientes.

	- Validar con un software los metadatos (no especificado)
Herramientas utilizadas en la pericia	No especifica el software utilizado para la extracción de metadatos.

Número de juicio	01803-2015-0055
Tema	Examinar el sistema ESIGEF de la Universidad de Cuenca. Generar los reportes necesarios para su posterior análisis.
Metodología aplicada	- Acceder a las opciones solicitadas junto a la persona que genero los reportes - Analizar el primer reporte que es el comprobante de pago - Analizar el tercer reporte el cual es la relación de pago y su estatus donde se ve el estado del pago al IESS, el cual consta como entregado
Herramientas utilizadas en la pericia	sistema ESIGEF de la Universidad de Cuenca para consultas al sistema.

Número de juicio	01283-2015-02042
Tema	Analizar el contenido de un CD que está dentro del proceso, dicho CD contiene un video
Metodología aplicada	Descriptiva: mirar el video, así como escuchar lo narrado dentro del mismo para en base a este análisis sacar las respectivas conclusiones.
Herramientas utilizadas en la pericia	Ninguna

Número de juicio	01333-2015-03689
Tema	La pericia solicitada consistió en realizar una reproducción de datos electrónicos de otro proceso.
Metodología aplicada	Pericia no realizada por falta de pago
Herramientas utilizadas en la pericia	Pericia no realizada

Número de juicio	01371-2015-00536
Tema	constatar que existe el usuario de la persona demandante tanto en el sistema QUIPUX, como en el sistema de reloj biométrico DATAACROM.
Metodología aplicada	1. Con los usuarios administradores se consultó los usuarios existentes en los sistemas. 2. En el caso del sistema DATAACROM, se accedió con el usuario LBERMEO que aún seguía activo
Herramientas utilizadas en la pericia	Sistema QUIPUX Sistema de reloj biométrico DATAACROM

Número de juicio	01371-2015-00623
Tema	Examinar el registro de marcaciones de la persona demandante durante el periodo en el que trabajó en la empresa Electro Éxito a la cual demanda.
Metodología aplicada	- Revisar el registro de marcaciones de la persona demandante. - Se verificó que se ejecuta un proceso de limpiado de información del reloj biométrico cada 2-3 meses
Herramientas utilizadas en la pericia	Reloj biométrico

Número de juicio	09359-2015-05149
Tema	Determinar la grabación que consta en la memoria telefónica que ha sido presentada y transcribirla.
Metodología aplicada	1. Disponer de la Micro SD - USB a ser analizada 2. Revisar el contenido de la memoria 3. Realizar una búsqueda minuciosa de cada carpeta 4. Utilizar el Software RECIVA para recuperar archivos de audio y video borrados
Herramientas utilizadas en la pericia	Software RECIVA para recuperación de archivos borrados

Número de juicio	01501-2014-0096
Tema	Revisar si existen o no obligaciones tributarias impagas, revisar dicha información solicitada en el sistema del SRI.
Metodología aplicada	- Se realizó las consultas solicitadas dentro del sistema de gestión de cobros de cada uno de los contribuyentes. - Al realizar la consulta se obtuvo un listado de obligaciones, la información más relevante que se muestra es el tipo de documento, la descripción del impuesto, periodo fiscal, monto, saldo.
Herramientas utilizadas en la pericia	Sistema de gestión de cobros del SRI

Número de juicio	03204-2017-00295
Tema	Análisis de un teléfono celular
Metodología aplicada	- Indicar el nombre de los contactos tanto de WhatsApp y Messenger de los cuales hay que realizar el informe pericial - Revisar las características del celular que fue entregado - Revisar la existencia de la conversación realiza
Herramientas utilizadas en la pericia	Plataformas de WhatsApp y Messenger

Número de juicio	09100-2016-00014
Tema	Experticia informática dispuesta a los registros informáticos en los sistemas internos de la compañía.
Metodología aplicada	Se aplicó método de la observación y análisis de los registros informáticos en los sistemas internos de la compañía TC Televisión, para recolectar la información se entrevistó a los funcionarios de la compañía que tiene acceso a la información requerida sobre el bloque o desactivación del usuario.
Herramientas utilizadas en la pericia	Sistema de correo de Google App Sistema de Active Directory de Windows Server 2012 Sistema financiero administrativo ERP

Número de juicio	09285-2016-00783
Tema	Verificar los sistemas y plataforma del integrador de la compañía TEAM SOURSINNG CIA LTADA
Metodología aplicada	Metodología basada en el flujo de procesos de OTECEL (empresa), que tiene que ver con el lanzamiento de un nuevo producto, la captación de clientes a través de sus promociones vía celular, la suscripción al servicio, el registro de la suscripción, la activación del servicio, los débitos realizados y la inactivación del servicio.
Herramientas utilizadas en la pericia	SMSC, este programa se encarga de subir los datos de aceptación del servicio, hacia el Sistema Informático de OTECEL denominado WAU. WAU, es un software desarrollado en ambiente web, es decir, que se puede tener acceso desde cualquier parte del mundo y corre en un sitio seguro.

Número de juicio	17811-2016-00262
Tema	Enlistar kits de grabación de tres unidades judiciales
Metodología aplicada	- Tomar fotografías a los kits para salas de grabación presentes en cada una de las salas de audiencia. - Ingresar al computador con la finalidad de ingresar al software CICERO, y poder verificar las audiencias que se encuentran grabadas. - Revisar el directorio VIDEOCICERO que contiene archivos de audio.
Herramientas utilizadas en la pericia	Software CICERO MySQL, usada por el software CICERO

Número de juicio	16331-2015-01285
Tema	Hacer una investigación de la cuenta agresora si tiene vínculo con el legitimado activo, de igual forma si en la fecha que se dio la agresión el legitimado tenía cuenta en el Facebook.
Metodología aplicada	- Solicitar información que tenga algún vínculo con la investigación solicitada. - Análisis de información

	- Validación de la información: a través de capturas de pantalla.
Herramientas utilizadas en la pericia	Plataforma de red social Facebook

Número de juicio	01283-2016-03612
Tema	Realizar la extracción de la información contenida en el celular marca Samnsung Galaxy S4, IMEI: 352603/06/455141/4, respecto a la grabación de video con el fin de que se determine la calidad de grabación y la calidad como el origen de los acontecimientos sucedidos.
Metodología aplicada	- Adquirir evidencia - Verificar IMEI - Extracción del grabado - Cumpliendo con la cadena de custodia, se procede a grabar los videos en el CD adjunto, certificando que éstos no han sido modificados, provienen de su origen y no podrán ser modificados en su contenido dentro del referido CD, puesto que están gravados con protección de escritura. - Determinar calidad de videos - Buscar las características técnicas de cada uno de los videos extraídos
Herramientas utilizadas en la pericia	Google Maps para determinar donde fueron grabados los videos.

Número de juicio	01333-2015-11088
Tema	Transcripción del audio de un CD
Metodología aplicada	- Identificar el formato - Se transcribió el contenido - Se realizó capturas de las imágenes del audio video
Herramientas utilizadas en la pericia	Ninguna

Número de juicio	01371-2016-00361
Tema	Realizar la revisión del correo electrónico del compareciente

Metodología aplicada	- Buscar los correos electrónicos - Verificar que corresponden en su contenido a los enviados por el compareciente - Firmarlos digitalmente indicando autenticidad
Herramientas utilizadas en la pericia	Servicio de correo electrónico corporativo en la aplicación Zimbra

Número de juicio	07333-2016-00364G
Tema	Revisión del sistema contable
Metodología aplicada	No se pudo realizar el peritaje, dado que los directivos estaban llegando a un acuerdo
Herramientas utilizadas en la pericia	No utilizadas

Número de juicio	09802-2017-00046
Tema	Verificar la existencia de los servicios de digitalización e indexación de los libros de propiedad, hipoteca, adjudicación, mercantil, industrial, demanda, embargos, compra venta, historia de dominio del registro de la propiedad del gobierno autónomo descentralizado municipal del cantón Durán.
Metodología aplicada	se utilizó el método de observación donde se recoge la información requerida 1. Inspección de los trabajos de digitalización e indexación 2. Reconocimiento en área de tecnología 3. Reconocimiento área de repertorio
Herramientas utilizadas en la pericia	No tiene almacenado ningún archivo o sistema relacionado con la contratación

Número de juicio	17151-2017-00295
Tema	Extraer del CD las fotografías y determinar la fecha en las que fueron tomadas
Metodología aplicada	- Conectar el USB al portatil - Determinar ubicación del archivo - Extraer los archivos .jpg

Herramientas utilizadas en la pericia	FTK Imager para generar la imagen forense y exportar los archivos de tipo fotográfico HashCalc para generar el código hash de los archivos Para la obtención de los metadatos: - JPGSNOOP - FOCA

Número de juicio	17230-2016-18207
Tema	Acceder al servidor de correos donde se encuentran los buzones mencionados o un respaldo digital válido de dicho servidor en el periodo que se generaron dichos correos
Metodología aplicada	No se logra acceder al servidor
Herramientas utilizadas en la pericia	No utilizadas.

Número de juicio	17151-2016-02433G
Tema	- Revisión del correo electrónico con la finalidad de determinar: - Recepción del correo. - Asunto, fecha y hora del email. - Autenticidad y a quién pertenece la dirección de email. - Contenido textual del email. - Personas a las que se les envío copia del correo. - Dirección IP del correo. - Dirección desde donde se emitió el correo electrónico.
Metodología aplicada	- Se inicia buscando el correo electrónico en el programa Hotmail. - Se realizó el cotejamiento de los distintos buzones con el correo electrónico objeto de la pericia. - Obtención de la cabecera del correo electrónico localizado. - Se analizó la cabecera del correo electrónico con la aplicación forense ToolBox Google y MxBoxTools para validar su autenticidad.
Herramientas utilizadas en la pericia	MXToolBox – Mxtools Analizer Head ToolBox Google

Número de juicio	17554-2017-00005
Tema	Desmaterialización del contenido de un CD
Metodología aplicada	- Análisis del CD, revisión de meta data - Identificar personas que intervienen en el video - Transcripción de video
Herramientas utilizadas en la pericia	No utilizadas

Número de juicio	18151-2016-00965
Tema	Realizar un peritaje sobre la información de suspensión, consumos y notificaciones realizadas a la línea 0993883701.
Metodología aplicada	- Obtener información de las llamadas, mensajes y consumos de datos realizados por el usuario. - Validar la información obtenida. - Capturar pantallas con datos que demuestren la información solicitada a CNT. - Exponer la información obtenida mediante informe.
Herramientas utilizadas en la pericia	Sistema comercial de la CNT denominada SmartFlex

Número de juicio	17302-2009-0357
Tema	Verificar el daño ocasionado en la red de planta externa de la operadora CNT E.P
Metodología aplicada	- Inspección en el lugar donde se realizó el daño de la red de CNT. - Verificación del reporte de daño de la red y consecuentemente la interrupción del servicio por parte de CNT e informado al Organismo de Control de Telecomunicaciones a la fecha de la interrupción. - Revisión del Informe de CNT, en la que se reporta que el daño fue ocasionado por una empresa subcontratista de la empresa TELMEX.
Herramientas utilizadas en la pericia	No utilizadas.

Número de juicio	17151-2016-02596G
Tema	Certificar la autenticidad, así como la dirección IP del correo electrónico enviado al Sr. Francisco Moreno el miércoles 05/10/2016 13:40
Metodología aplicada	- Se inicia buscando los correos electrónicos en el programa Outlook. - Se realizó el cotejamiento de los distintos buzones con el correo electrónico objeto de la pericia. - Obtención de la cabecera del correo electrónico localizado en el programa Outlook. - Se analizó la cabecera del correo electrónico con la aplicación forense ToolBox Google y MxBoxTools para validar su autenticidad.
Herramientas utilizadas en la pericia	Mxtools Analizer Head Microsoft Outook

Número de juicio	01283-2017-00860
Tema	Extracción de la información del Memory Flash
Metodología aplicada	- Obtener una descriptiva detallada de la información que se encuentra en el dispositivo entregado - Generar identificadores únicos de la información para que puedan ser cotejados en peritajes similares.
Herramientas utilizadas en la pericia	No utilizada

Número de juicio	03283-2017-00506
tema	Extraer información de correo electrónico
Metodología aplicada	Resumir la información extraída de cada uno de los correos electrónicos de las cuentas involucradas.
Herramientas utilizadas en la pericia	Mxtools Analizer Head Generador de código Hash no especificado.

Número de juicio	01371-2017-00404

Tema	Determinar la marcación del actor en el reloj biométrico
Metodología aplicada	- Realizar la revisión y levantamiento de información en la matriz de la empresa Diario el Tiempo - Entrevista con la responsable/administradora del sistema biométrico - Análisis del equipo mediante el cual se administra el sistema biométrico - Análisis y auditoría del aplicativo-software que gestiona el sistema biométrico
Herramientas utilizadas en la pericia	Sistema de Administración de Tiempo y Asistencia V4.5.1" – de ANVIZ Biometric Tech

Número de juicio	14256-2017-00163G
Tema	Evidenciar la desmaterialización, impresión y certificación de todos los documentos particularizados
Metodología aplicada	Para analizar la prueba pericial informática se ha aplicado el método científico (informático) y las técnicas de observación, experimentación, obtención y análisis de la información.
Herramientas utilizadas en la pericia	Servidor de correo electrónico Zimbra

Número de juicio	17230-2016-09283
Tema	Inspección judicial
Metodología aplicada	Verificación física, de las instalaciones de los equipos del Estudio compuesto por el Centro de emisión automatizado de programación
Herramientas utilizadas en la pericia	No utilizadas

Número de juicio	17151-2016-00574
Tema	Extracción y transcripción de audio CD

Metodología aplicada	Verificar el CD entregado por la parte que demanda, encontrándose con 9 archivos de audio en formato 3GPP y convertirlo a formato MP3.
Herramientas utilizadas en la pericia	Windows Media

Número de juicio	17811-2016-01506
Tema	Comprobar la existencia de los instaladores del Sistema Integrado de Gestión Municipal ERP CABILDO
Metodología aplicada	- Realizar una copia de los instaladores del Sistema Integrado de Gestión Municipal ERP CABILDO - Evidenciar todos los módulos instalados en el Sistema Integrado de Gestión Municipal ERP CABILDO - Comprobar y evidenciar, que se encuentra instalado el motor de la Base de Datos ORACLE - Verificar que existe un crecimiento de la Base de Datos - Verificación y establecimiento del detalle de transacciones existentes en la base de datos en todos los módulos del programa informático CABILDO instalado en el GAD Cayambe
Herramientas utilizadas en la pericia	Toad for Oracle

Número de juicio	17231-2017-00324
Tema	Determinar titular, administrador y usuarios que manipulan el sistema MAGAYA
Metodología aplicada	- Reuniones mantenidas para la recopilación de la información - Información primaria recopilada y verificada
Herramientas utilizadas en la pericia	Sistema local MAGAYA

Número de juicio	17204-2014-1645
Tema	Extracción de audio y video
Metodología aplicada	- Recolección de información

	- Transcripción por medio de herramientas.
Herramientas utilizadas en la pericia	Groove Music de la empresa Microsoft Transcritos y editados usando el programa informático Microsoft Word

Número de juicio	06010-1815-070206
Tema	Realizar la pericia informática en la Plataforma ENGOLDEX/ON LINE GLOBAL INTERGOLD.
Metodología aplicada	se empezó identificando el problema central, es decir la existencia o no de la empresa ENGOLDEX/ONLINE GLOBAL INTERGOLD, así como también comprobar la existencia de los clientes en la Plataforma Virtual y cuál es el modus operandi de la empresa en mención; mismos que a través del método de deducción lógica se logró identificar los hechos para la comprobación de la hipótesis.
Herramientas utilizadas en la pericia	Navegador de internet Google Chrome Plataforma de Global Inter Gold

Número de juicio	17371-2016-00673
Tema	Extraer información de correo electrónico
Metodología aplicada	- Recopilación de información, claves facilitadas - Verificar información - Comprobar intercambio de mensajes por medio del correo electrónico
Herramientas utilizadas en la pericia	Servicio de correo electrónico de Outlook

Número de juicio	01371-2016-00539
Tema	Verificar el funcionamiento del Reloj Biométrico y constatar que consta la huella digital del demandante
Metodología aplicada	- Acudir a la empresa denunciada - Verificar existencia del dispositivo - Revisión del funcionamiento del reloj biométrico

	- Ejecución del software de control y del dispositivo - Revisión de usuarios
Herramientas utilizadas en la pericia	Reloj biométrico ANVIZ EP Series

Número de juicio	01283-2016-02601
Tema	- Determinar si la cuenta, blog o dirección electrónica es personal: http://jcelobservador.blogspot.com - Determinar si la página web, dirección electrónica Milhojas.is/61242-la-ruta-criminal.del-oro-ecuatoriano-html es real e identifica quien más compartieron. - Determinar si la página web es real e identificar de la noticia y publicación. http://www.vericesnews.com
Metodología aplicada	No se utiliza
Herramientas utilizadas en la pericia	https://www.elhacker.net/ para revisar la ubicación geográfica

Número de juicio	06282-2016-03689G
Tema	Reconocimiento informático de las siguientes direcciones de las redes sociales: a) https://www.facebook.com/No-más-injusticias (con el seudónimo. y, b) https://www.facebook.com/profile.php?id=100014044235907&fref=ts
Metodología aplicada	- Identificar las páginas de Facebook - Obtener información contenida en las páginas identificadas
Herramientas utilizadas en la pericia	No utilizadas

Número de juicio	01331-2016-00650
Tema	Resultados de la experticia realizada en los equipos de computación que se encuentran en las Oficinas de WESTERN UNION de Gualaceo
Metodología aplicada	Para analizar la prueba pericial informática se ha aplicado el método científico (informático) y las técnicas de observación, experimentación, obtención y análisis de la información.

Herramientas utilizadas en la pericia	Sistema informático denominado “Cajas” Visual Basic 6.0. Access: Base de datos

Número de juicio	06335-2017-00064
Tema	Transcripción de los correos electrónicos de la cuenta electrónica del actor
Metodología aplicada	- Ingresar a la cuenta de correo electrónico del actor - Buscar correos de interés - Transcribir correos de interés
Herramientas utilizadas en la pericia	Outlook Mail

Número de juicio	17316-2017-00064
Tema	Revisión de reporte en reloj biométrico, y sistemas de almacenamiento de información y recuperación
Metodología aplicada	Se revisa el reloj biométrico. Se revisa el procedimiento de ingreso de un nuevo empleado. Se obtiene información del reloj biométrico. Se solicita información de los sistemas informáticos manejados por la Jefatura de Recursos Humanos y Jefatura de Sistemas.
Herramientas utilizadas en la pericia	Software que maneja el reloj biométrico (No especificado)

Número de juicio	17811-2016-01772
Tema	Determinar la autenticidad de un correo electrónico, fecha de envío, si el correo electrónico realmente fue o no remitido al correo electrónico ciataxecurep@yahoo.com.
Metodología aplicada	- Se inicia ingresando al Centro de Administración del Exchange. - Se realiza la búsqueda del usuario María de los Ángeles Herrera Villalva.

	- Se realizó el cotejamiento del correo electrónico que se solicita en el expediente.
Herramientas utilizadas en la pericia	Servidor de correo electrónico empresarial Exchange ToolBox Google

Número de juicio	03283-2016-00477
Tema	Obtener información que salió de la red social FACEBOOK de la conversación entre el demandante y demandado
Metodología aplicada	- Acceder a las cuentas de los involucrados - Se procede a obtener las capturas de pantalla de las conversaciones mantenidas entre los usuarios de Facebook
Herramientas utilizadas en la pericia	Facebook

Número de juicio	06352-2017-00063
Tema	Determinar la existencia y ubicación del reloj biométrico. 2.- Que la memoria o CPU no ha sido manipulada o alterada. 3.- Las horas de ingreso y salida de la empleada X
Metodología aplicada	Para claridad en la exposición ésta pericia divide el análisis en 3 apartados congruentes con cada uno de los requerimientos: - La existencia y ubicación del reloj biométrico. - Que la memoria o CPU no ha sido manipulada o alterada. - Las horas de ingreso y salida de la empleada María Augusta Cano León desde el 05 de junio del 2014 al 02 de febrero del 2017, incluidos los sábados.
Herramientas utilizadas en la pericia	Para descargar la información del reloj biométrico se utiliza el software ZKTime5.0.

La información de todos estos informes se ha tabulado en la matriz de datos que se muestra a seguir y de la que se extraerán los resultados de este estudio de campo.

NO.	JUICIO	UNIDAD JUDICIAL	TIPO DE DELITO- ACCION O INFRACCION	OBJETO (TEMA) PERICIA	AMBIENTE QUE SE IDENTIFICA LA EVIDENCIA	DESCRIPCION DE LA EVIDENCIA	APLICA METODOLOGIA, TECNICA O PROCESO FORENSE
1	14304-2018-00313	MULTICOMPETENTE	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 1	DETERMINAR ORIGEN DE MENSAJE DE UNA CUENTA DE FACEBOOK Y CORROBORAR EXISTENCIA DE PUBLICACIÓN.	RED SOCIAL INTERNET	FACEBOOK	SI
2	17811-2016-00262	CONTENCIOSO ADMINISTRATIVO	SUBJETIVO	VERIFICAR SUMINISTROS INFORMÁTICOS ENTREGADOS	INSPECCION LOCAL	INSPECCION	NO
3	07257-2018-00171	MULTICOMPETENTE	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 1	VERIFICAR MENSAJES Y VIDEOS EN FACEBOOK	RED SOCIAL INTERNET	FACEBOOK	NO
4	11333-2015-05689	CIVIL	COBRO DE DINERO	VERIFICAR AUTENTICIDAD DE CORREPS ELECTRONICOS Y DESCARGARLOS	APLICACIÓN INTERNET	MICROSOFT OUTLOOK	NO
5	01618-2017-00148	MULTICOMPETENTE	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 1	EXTRACCION DE INFORMACION DE MEDIO DIGITAL	MEDIO FISICO	SERVIDOR FISICO	SI
6	01283-2018-01072	PENAL	182 CALUMNIA	TRANSCRIPCION DE AUDIO Y VIDEO	MEDIO FISICO	CAMARA EQUIPO CELULAR MOVIL	SI
7	01283-2018-01297	PENAL	182 CALUMNIA	IDENTIFICAR PERFIL DE QUIEN PUBLICÓ MENSAJES OFENSIVOS	RED SOCIAL INTERNET	FACEBOOK	SI
8	01283-2018-02993G	PENAL	187 ABUSO DE CONFIANZA, INC.1	VERIFICAR PERFIL DE FACEBOOK Y RESPALDAAR IMÁGENES Y MENSAJES	RED SOCIAL INTERNET	FACEBOOK	NO
9	03332-2017-00565	CIVIL	PAGO DE HABERES	EXTRAER VIDEO DE TELEFONO CELULAR	MEDIO FISICO	CAMARA EQUIPO CELULAR MOVIL	SI
10	01283-2018-00098	PENAL	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 4	TRANSCRIBIR GRABACIONESDE AUDIO Y VIDEO	MEDIO FISICO	CD	NO
11	17371–2017–05550	TRABAJO	INDEMINZACION POR DESPIDO INTESPESTIVO	AANALISIS DE ARCHIVOS	MEDIO FISICO	CD	NO
12	18371-2018-00154	TRABAJO	INDEMINZACION POR DESPIDO INTESPESTIVO	EXTRAER DATOS DE GPS	MEDIO FISICO	GPS	SI
13	03203-2018-00254	FAMILIA, MUJER,NIÑEZ	INVENTARIO DE SOCIEDAD CONYUGAL	ANALISIS DEL CONTENIDO DE CD	MEDIO FISICO	CD	NO
14	17308-2011-1444	CIVIL	ORDINARIO	VERIFICACION DE EXUSTENCIA DE HARDWARE Y SOFTWARE	MEDIO FISICO	SERVIDOR FISICO	NO
15	11282-2017-01313	PENAL	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 4	EXTTACCION Y ANALISES DE VIDEOS	MEDIO FISICO	SERVIDOR FISICO	NO
16	11282-2017-00739	PENAL	182 CALUMNIA	ANALIS Y EXTRACCION DE ARCHIVOS	MEDIO FISICO	DISCO EXTERNO	NO
17	15301-2017-01000	CIVIL	COBRO LETRA DE CAMBIO	TRANSCRIPCION DE AUDIOS	MEDIO FISICO	CD	NO
18	11203-2017-03613	FAMILIA, MUJER,NIÑEZ	DIVORCIO POR CAUSAL	VERIFICACION Y ANALISIS DE LLAMADAS	MEDIO FISICO	CELULAR	NO
19	17294-2018-00101	PENAL	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 1	DETERMINAR PERFILES DE FACEBOOOK Y TWITTER	RED SOCIAL INTERNET	FACEBOOK TWITTER	NO
20	17811-2016-00262	CONTENCIOSO ADMINISTRATIVO	SUBJETIVO	VERIFICACION Y EXTRACCION DE DOCUEMNTOS EN SITIO WEB	APLICACIÓN INTERNET	WEB	NO
21	06335-2016-00567	CIVIL	COBRO DE PAGARÉ A LA ORDEN	EVALUO DE EQUIIPOS	MEDIO FISICO	SERVIDOR FISICO	NO
22	07331-2015-00190	MULTICOMPETENTE	PRESCRIPCIÓN ADQUISITIVA DE DOMINIO	VERIFICACION DE IMÁGENES	APLICACIÓN INTERNET	GOOGLE	NO
23	05254-2017-00211	PENAL	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 1	VERIFICAR Y EXTRAER PUBLICACION	RED SOCIAL INTERNET	FACEBOOK INSTAGRAM	NO
24	07331-2018-00092	MULTICOMPETENTE	DESPOJO VIOLENTO	EXTRAER CONTENIDOS	MEDIO FISICO	DISCO EXTERNO	NO
25	17811-2015-01595	CONTENCIOSO ADMINISTRATIVO	SUBJETIVO	VERIFICAR EXISTENCIA DE EQUIPOS	INSPECCION LOCAL	INSPECCION	NO
26	17811-2016-00268	CONTENCIOSO ADMINISTRATIVO	SUBJETIVO	VERIFICAR EXISTENCIA DE EQUIPOS	INSPECCION LOCAL	INSPECCION	NO
27	01283-2016-03420	PENAL	152 LESIONES, NUM. 2	EXTRACCION DE INFORMACION CUENTA FACEBOOK	RED SOCIAL INTERNET	FACEBOOK	NO
28	01331-2017-00189	CIVIL	COBRO LETRA DE CAMBIO	VERIFICACION DE LOGS SISTEMA INFORMATICO	MEDIO FISICO	SERVIDOR LOCAL	NO
29	07307-2017-00308	CIVIL	COBRO DE PAGARÉ A LA ORDEN	VERIFICACION DE LOGS SISTEMA INFORMATICO	MEDIO FISICO	SERVIDOR	NO
30	09285-2014-2449	PENAL	INJURIA	EXTRACCION DE MENSAJES TWITTER	RED SOCIAL INTERNET	TWITTER	NO
31	09284-2013-0175	PENAL	ART.75 ENTREGA DEL BIEN O PRESTACIÓN DEL SERVICIO.	VERIFCACION DE LOGS DE SISTEMA	MEDIO FISICO	SISTEMA LOCAL	NO
32	07333-2015-0306	CIVIL	REQUERIMIENTO JUDICIAL	AUTENTICIAD DE CORREOS ELECTRÓNICOS	APLICACIÓN INTERNET	OUTLOOK	NO
33	01371-2015-0138	TRABAJO	PAGO DE HABERES	EXTRACCIÓN DE CORREOS ELECTRONICOS	MEDIO FISICO	SERVIDOR LOCAL	NO
34	01371-2015-00351	TRABAJO	PAGO DE HABERES	EXTRACCIÓN DE CORREOS ELECTRONICOS	MEDIO FISICO	SERVIDOR LOCAL	SI
35	01371-2015-00435	TRABAJO	PAGO DE HABERES	AUTENTICIAD DE CORREOS ELECTRÓNICOS	APLICACIÓN INTERNET	GMAIL	NO
36	09354-2014-0702	TRABAJO	PAGO DE HABERES	VERIFICACION DE LOGS SISTEMA INFORMATICO	MEDIO FISICO	SERVIDOR LOCAL	NO
37	01371-2015-00538	TRABAJO	PAGO DE HABERES	VERIFICACION DE LOGS SISTEMA INFORMATICO	MEDIO FISICO	SERVIDOR LOCAL	NO
38	01371-2015-00761	TRABAJO	INDEMINZACION POR DESPIDO INTESPESTIVO	VERIFICACION DE LOGS SISTEMA INFORMATICO	MEDIO FISICO	SERVIDOR LOCAL	NO
39	01801-2012-0392	CONTENCIOSO ADMINISTRATIVO	SUBJETIVO	VERIFICACION DE LOGS SISTEMA INFORMATICO	MEDIO FISICO	SERVIDOR LOCAL	NO
40	11333-2014-2923	CIVIL	ART. 486 CODIGO DE COMERCIO ART. 413.CPC.	TRANSCRIPCION DE CONTENIDOS	MEDIO FISICO	CD	NO
41	13331-2016-00160	CIVIL	COBRO PAGARE A LA ORDEN	INSPECCION DE EQUIPOS ELECTRÓNICOS	APLICACIÓN INTERNET	VISITA AL SITIO	NO
42	17151-2017-00137	PENAL	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 1	EXTRACION DE MENSAJES WHATSAPP	RED SOCIAL INTERNET	WHATSAPP	NO
43	17113-2014-3252	PENAL	NULIDAD DE INSTRUMENTO PÚBLICO	TRANSCRIPCCIÓN DE AUDIO	APLICACIÓN INTERNET	INTERNET	NO
44	17811-2015-01239	CONTENCIOSO ADMINISTRATIVO	PIRATERIA	EVALUAR EQUIPO DE DECODIFICADOR	INSPECCION LOCAL	INSPECCION FISICA	SI
45	11333-2013-14637	CIVIL	486 CODIGO DE COMERCIO ART. 413.CPC.	AVALUO DE EQUIPOS	INSPECCION LOCAL	INSPECCION FISICA	NO
46	07331-2017-00443	CIVIL	DESPOJO VIOLENTO	EXTRACCION DE CONTENIDOS	MEDIO FISICO	CD	NO
47	07307-2015-00354	CIVIL	INCUMPLIMIENTO DE CONTRATO	VERIFICACION DE SISTEMA INFORMATICO	MEDIO FISICO	SERVIDOR LOCAL	NO
48	09359-2015-04009	TRABAJO	INDEMNIZACIÓN POR DESPIDO INTEMPESTIVO	EXTRACCION DE INFORMACION	MEDIO FISICO	DISCO EXTERNO	SI
49	10333-2016-00560	CIVIL	COBRO LETRA DE CAMBIO	VERIFICACION MENSAJES FACEBOOK	RED SOCIAL INTERNET	FACEBOOK	NO
50	07281-2017-00009	PENAL	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 4	VERIFICACION DE AUTENTICIDAD DE CONTENIDOS	MEDIO FISICO	CD	NO
51	10333-2016-00560	CIVIL	PRESCRIPCIÓN ADQUISITIVA DE DOMINIO	VERIFICACIÓN DE LA CONVERSACIÓN POR LA RED SOCIAL	RED SOCIAL INTERNET	FACEBOOK	NO
52	07281-2017-00009	PENAL	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 4	TRANSCRIPCION DE AUDIO Y VIDEO	MEDIO FISICO	CD	NO
53	13311-2015-00464		NO SE ENCUENTRA PROCESO	TRANSCRIOCION DE AUDIO Y VIDEO	MEDIO FISICO	CD/DVD-R	NO
54	13337-2016-01224	CIVIL	COBRO DE LETRA DE CAMBIO	EXTRACCIÓN DE LAS CONVERSACIONES MANTENIDAS POR FACEBOOK	RED SOCIAL INTERNET	FACEBOOK	SI

55	03371-2015-00484		NO SE ENCUENTRA PROCESO	REVISAR LA BITÁCORA DE INGRESO Y SALIDA DEL PERSONAL	MEDIO FISICO	SISTEMA LOCAL	NO
56	17230-2015-16900	CIVIL	REINVINDICACIÓN	EXTRACCION Y ANALISIS DE CORREOS ELECTRONICOS	APLICACIÓN INTERNET	OUTLOOK	SI
57	17293-2017-00535	PENAL	182 CALUMNIA	EXTRACCION DE INFORMACION DE LA PAGINA DE LA FISCALIA	APLICACIÓN INTERNET	INTERNET	NO
58	01604-2014-0354	CIVIL	DAÑO MORAL	REVISION DE EXISTENCIA DE DOCUMENTOS EN SISTEMA	MEDIO FISICO	SISTEMA LOCAL	NO
59	01802-2014-0205	CONTENCIOSO ADMINISTRATIVO	SUBJETIVO	EXAMINAR METADATOS DE DOCUMENTOS	MEDIO FISICO	NAVEGADOR DE ARCHIVOS	NO
60	01803-2015-0055	CONTENCIOSO ADMINISTRATIVO	SUBJETIVO	EXAMINAR EL SISTEMA LOCAL Y REPORTAR ANOMALIAS	MEDIO FISICO	SISTEMA LOCAL	NO
61	01283-2015-02042	PENAL	DERECHOS FUNDAMENTALES DEL CONSUMIDOR	ANALIZAR CONTENIDO DE CD	MEDIO FISICO	NINGUNA	NO
62	01333-2015-03689	CIVIL	RECUSACIÓN	REPRODUCCION DE DATOS ELECTRONICOS	MEDIO FISICO	NO REALIZADO	NO
63	01371-2015-00536	TRABAJO	PAGO DE HABERES LABORALES	ANALIZAR SISTEMA DE RELOJ BIOMETRICO	MEDIO FISICO	DATAACROM (SIST. RELOJ BIOMETRICO)	NO
64	01371-2015-00623	TRABAJO	PAGO DE HABERES LABORALES	REVISAR REGISTRO DE MARCACION DE ASISTENCIA	MEDIO FISICO	SISTEMA LOCAL	NO
65	09359-2015-05149	TRABAJO	INDEMNIZACIÓN POR DESPIDO INTEMPESTIVO	TRANSCRIBIR GRABACION DE MEMORIA TELEFONICA	MEDIO FISICO	SOFTWARE RECUVA	NO
66	01501-2014-0096	CONTENCIOSO TRIBUTARIO	IMPUGNACIÓN CONTRA RESOLUCIÓN DE LAS ADMINISTRACIONES TRIBUTARIAS	REVISION DE SISTEMA DE SRI	INSPECCION LOCAL	SISTEMA LOCAL	NO
67	03204-2017-00295	MULTICOMPETENTE	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 1	ANALISIS DE TELEFONO CELULAR	RED SOCIAL INTERNET	WHATSAPP	NO
68	09100-2016-00014	PRESIDENCIA GUAYAQUIL	PAGO DE HABERES LABORALES	EXTRAER REGISTROS DEL SISTEMA INTERNO	INSPECCION LOCAL	ACTIVE DIRECTORY DE WINDOWS	NO
69	09285 2016 00783	PENAL	DERECHOS FUNDAMENTALES DEL CONSUMIDOR	VERIFICAR LOS SISTEMAS Y PLATAFORMA DEL INTEGRADOR	INSPECCION LOCAL	SMSC/WAU	NO
70	17811-2016-00262	CONTENCIOSO ADMINISTRATIVO	SUBJETIVO	ENLISTAR HARDWARE	INSPECCION LOCAL	SOFTWARE CICERO	NO
71	16331-2015-01285	CIVIL	ACCIÓN DE PROTECCIÓN	REVISAR CUENTA AGRESORA EN FACEBOOK	RED SOCIAL INTERNET	FACEBOOK	NO
72	01283-2016-03612	PENAL	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 1	REVISAR GRABACION DE TELEFONO CELULAR	APLICACIÓN INTERNET	GOOGLEMAPS	SI
73	01333-2015-11088	CIVIL	ORDINARIO	TRANSCRIPCIÓN DEL AUDIO DE UN CD	MEDIO FISICO	NINGUNA	NO
74	01371-2016-00361	TRABAJO	PAGO DE HABERES LABORALES	REALIZAR LA REVISIÓN DEL CORREO ELECTRÓNICO DEL COMPARECIENTE	APLICACIÓN INTERNET	ZIMBRA	NO
75	07333-2016-00364G	CIVIL	INSPECCIÓN JUDICIAL	REVISIÓN DEL SISTEMA CONTABLE	INSPECCION LOCAL	NINGUNA	NO
76	09802-2017-00046	CONTENCIOSO ADMINISTRATIVO	DEPRECATORIO	VERIFICAR ESTADO DE LA PROPIEDAD EN SISTEMA MUNICIPAL	INSPECCION LOCAL	SISTEMA LOCAL	NO
77	17151-2017-00295	PENAL	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 4	ANALIZAR FOTOGRAFIAS EN CD	MEDIO FISICO	CD/FTK	SI
78	17230-2016-18207	CIVIL	FACTURAS	ACCEDER AL SERVIDOR DE CORREOS EMPRESARIAL	APLICACIÓN INTERNET	NINGUNA(NO REALIZADA)	NO
79	17151-2016-02433G	PENAL	SOLICITUD DE OFICIO	ANALISIS DE CORREO ELECTRONICO	APLICACIÓN INTERNET	MXTOOLBOX	NO
80	17554-2017-00005	PENAL	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 4	DESMATERIALIZACIÓN DEL CONTENIDO DE UN CD	MEDIO FISICO	CD	NO
81	18151-2016-00965	CONTRAVENCIONES	DERECHOS FUNDAMENTALES DEL CONSUMIDOR	ANALIZAR CONSUMOS REALIZADOS POR LINEA TELEFONICA	INSPECCION LOCAL	SISTEMA LOCAL	NO
82	17302-2009-0357	CIVIL	DINERO	VERIFICAR DAÑO EN RED	INSPECCION LOCAL	NINGUNA	NO
83	17151-2016-02596G	PENAL	SOLICITUD DE PERITAJE	VERIFICAR AUTENTICIDAD DE CORREPS ELECTRONICOS Y DESCARGARLOS	APLICACIÓN INTERNET	OUTLOOK	NO
84	01283-2017-00860	PENAL	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 1	EXTRACCIÓN DE LA INFORMACIÓN DEL MEMORY FLASH	MEDIO FISICO	PENDRIVE	NO
85	03283-2017-00506	PENAL	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 1	EXTRAER INFORMACIÓN DE CORREO ELECTRÓNICO	APLICACIÓN INTERNET	MXTOOLS/GENERADOR DE CODIGO HASH	SI
86	01371-2017-00404	TRABAJO	PAGO DE HABERES LABORALES	DETERMINAR LA MARCACIÓN DEL ACTOR EN EL RELOJ BIOMÉTRICO	INSPECCION LOCAL	SISTEMA LOCAL	NO
87	14256-2017-00163G	MULTICOMPETENTE	INSPECCIÓN PREPARATORIA	EVIDENCIAR LOS DOCUMENTOS DE CORREOS ELECTRONICOS	APLICACIÓN INTERNET	ZIMBRA	NO
88	17230-2016-09283	CIVIL	DAÑOS Y PERJUICIOS	INSPECCIÓN JUDICIAL	INSPECCION LOCAL	NINGUNA	NO
89	17151-2016-00574	PENAL	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 1	EXTRACCIÓN Y TRANSCRIPCIÓN DE AUDIO CD	MEDIO FISICO	WINDOWS MEDIA	NO
90	17811-2016-01506	CONTENCIOSO ADMINISTRATIVO	SUBJETIVO	VERIFICAR INSTALADORES DEL ERP DEL MUNICIPIO	INSPECCION LOCAL	TOAD FOR ORACLE	SI
91	17231-2017-00324	CIVIL	DAÑOS Y PERJUICIOS	DETERMINAR ADMINISTRADORES DE SISTEMA LOCAL	INSPECCION LOCAL	SISTEMA LOCAL	NO
92	17204-2014-1645	FAMILIA, MUJER,NIÑEZ	DIVORCIO POR MUTUO CONSENTIMIENTO	EXTRACCION DE AUDIO Y VIDEO	MEDIO FISICO	GROOVE MUSIC	NO
93	06010-1815-070206		NO SE ENCUENTRA PROCESO	ANALIZAR PLATAFORMA EMPRESARIAL	APLICACIÓN INTERNET	INTERNET	NO
94	17371-2016-00673	TRABAJO	PAGO DE HABERES LABORALES	EXTRAER INFORMACIÓN DE CORREO ELECTRÓNICO	APLICACIÓN INTERNET	OUTLOOK	NO
95	01371-2016-00539	TRABAJO	INDEMNIZACIÓN POR DESPIDO INTEMPESTIVO	CONSTATAR EXISTENCIA DE HUELLA EN RELOJ BIOMETRICO	INSPECCION LOCAL	SISTEMA BIOMETRICO ANVIZ	NO
96	01283-2016-02601	PENAL	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 1	ANALIZAR CUENTAS EN REDES SOCIALES	RED SOCIAL INTERNET	BLOGSPOT	NO
97	06282-2016-03689G		NO SE ENCUENTRA PROCESO	RECONOCIMIENTO DE DIRECCIONES URL	RED SOCIAL INTERNET	FACEBOOK	NO
98	01331-2016-00650	CIVIL	COBRO DE LETRA DE CAMBIO	ANALISIS DE EQUIPOS INFORMATICOS	INSPECCION LOCAL	SISTEMA LOCAL	NO
99	06335-2017-00064	CIVIL	DOCUMENTOS	TRANSCRIPCION DE CORREOS ELECTRONICOS	APLICACIÓN INTERNET	OUTLOOK	NO
100	17316-2017-00064	TRABAJO	PAGO DE HABERES LABORALES	REVISION Y EXTRACCION DE INFORMACION DEL SISTEMA BIOMETRICO	MEDIO FISICO	SISTEMA LOCAL	NO
101	17811-2016-01772	CONTENCIOSO ADMINISTRATIVO	SUBJETIVO	DETERMINAR AUTENTICIDAD DE CORREO ELECTRONICO	APLICACIÓN INTERNET	OUTLOOK EXCHANGE	NO
102	03283-2016-00477	PENAL	396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 1	ANALIZAR CONVERSACION DE RED SOCIAL FACEBOOK	RED SOCIAL INTERNET	FACEBOOK	NO
103	06352-2017-00063	TRABAJO	PAGO DE HABERES LABORALES	REVISAR MANIPULACIONES EN SISTEMA LOCAL	INSPECCION LOCAL	SISTEMA LOCAL	SI

Tabla 19: Matriz de datos

Análisis de resultados

Las unidades judiciales o juzgados que requieren pericias informáticas son los siguientes:

Tabla 20: Unidades Judiciales que Requieren Pericias Informáticas

UNIDAD JUDICIAL	Cuenta de UNIDAD JUDICIAL	PORCENTAJE
CIVIL	28	27%
CONTENCIOSO ADMINISTRATIVO	12	12%
CONTENCIOSO TRIBUTARIO	1	1%
CONTRAVENCIONES	1	1%
FAMILIA, MUJER, NIÑEZ	3	3%
MULTICOMPETENTE	7	7%
PENAL	28	27%
PRESIDENCIA GUAYAQUIL	1	1%
TRABAJO	18	17%
NO IDENTIFICADO	4	4%
TOTAL	103	100%

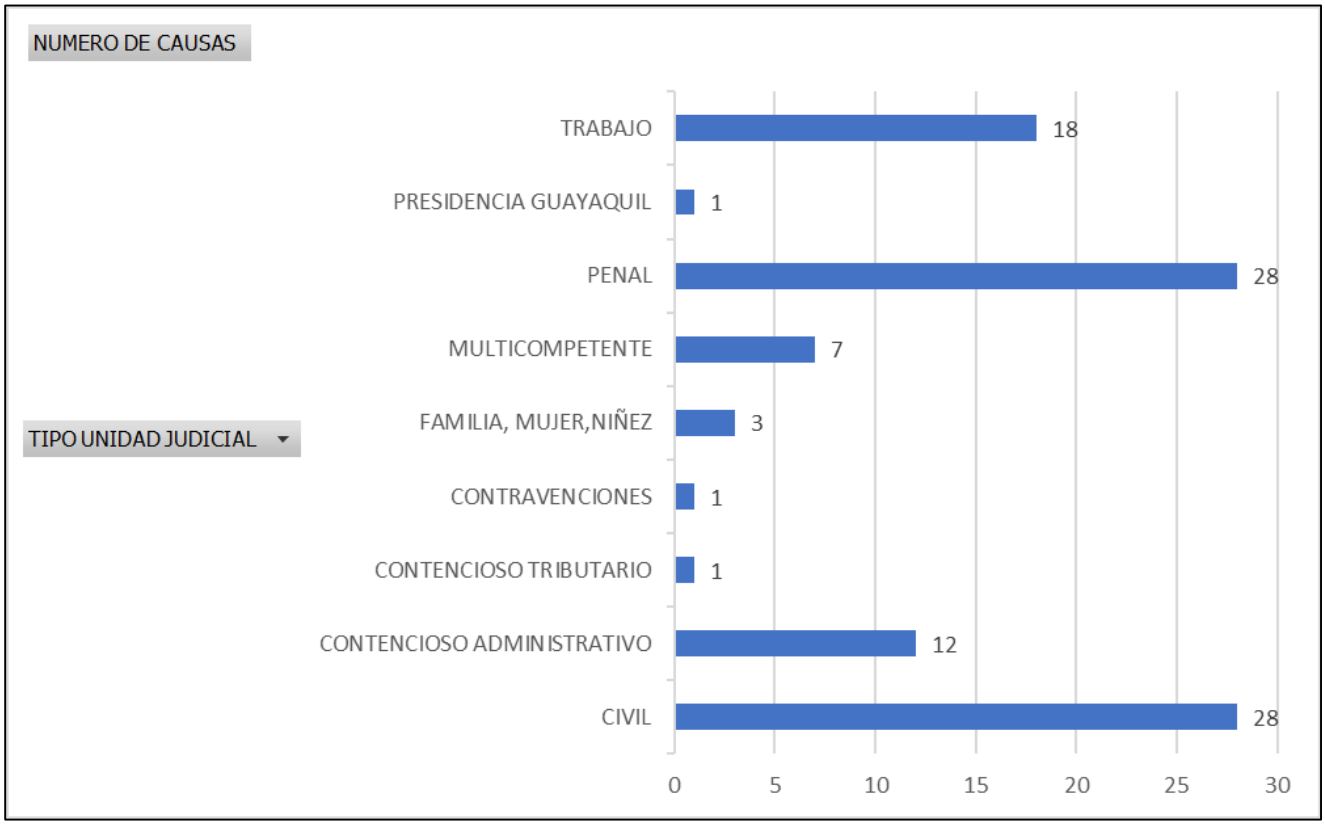


Figura 16: Causas por Tipo de Unidad Judicial

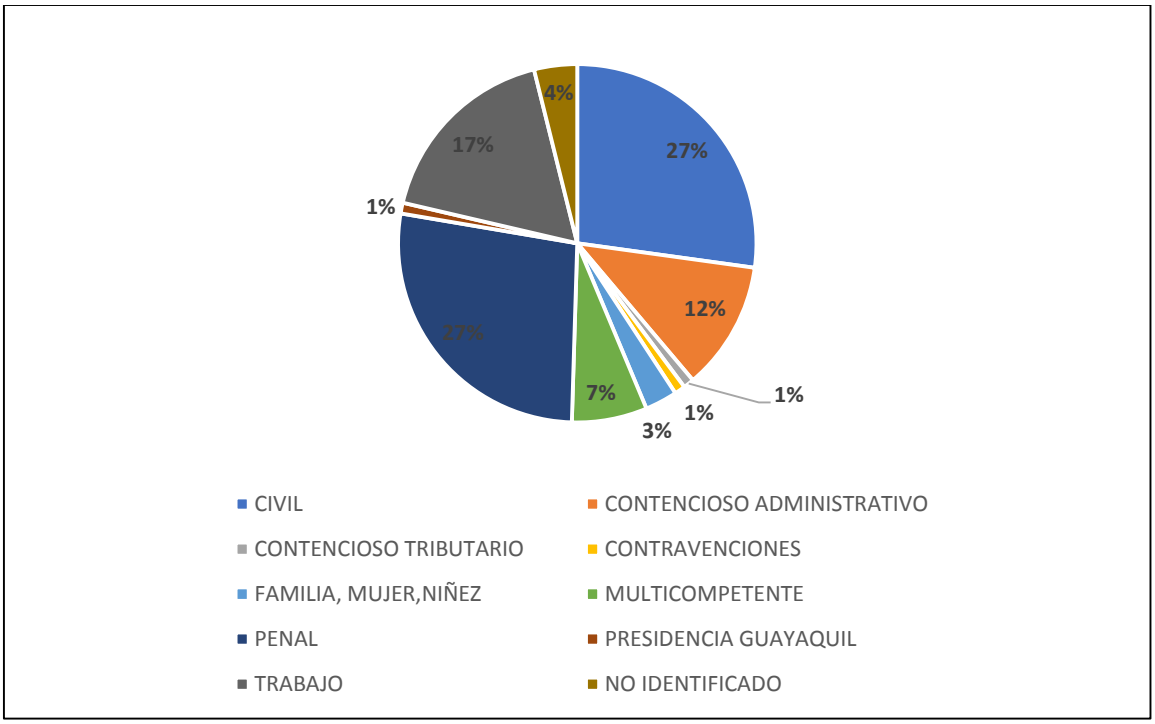


Figura 17: Pericias de Causas por Unidad Judicial

A pesar de que el desarrollo que se hizo en el capítulo cuatro se orientó a identificar y clasificar los delitos cibernéticos asociados al Código Orgánico Integral Penal (COIP), del análisis a los informes periciales se determina que la influencia de las TICs está también en otros ámbitos como se muestra en el detalle de las causas judiciales.

De los informes periciales analizados se determina que Las unidades de lo Civil, Trabajo, Niñez mujer y Adolescencia, Contencioso, Unidades Multicompetentes son las que principalmente solicitan pericias técnicas informáticas sobre TICs.

Tabla 21: Tipo de Delitos que Presentan Evidencias Digitales al Momento del Juzgamiento

396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 1	13
SUBJETIVO	10
PAGO DE HABERES LABORALES	8
NO SE ENCUENTRA PROCESO	6
PAGO DE HABERES	6
396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 4	6
COBRO LETRA DE CAMBIO	5
182 CALUMNIA	4
INDEMINZACION POR DESPIDO INTESPESTIVO	3
COBRO DE PAGARÉ A LA ORDEN	3

DERECHOS FUNDAMENTALES DEL CONSUMIDOR	3
INDEMNIZACIÓN POR DESPIDO INTEMPESTIVO	3
ORDINARIO	2
DESPOJO VIOLENTO	2
PRESCRIPCIÓN ADQUISITIVA DE DOMINIO	2
ART. 486 CODIGO DE COMERCIO ART. 413.CPC.	2
DAÑOS Y PERJUICIOS	2
INVENTARIO DE SOCIEDAD CONYUGAL	1
DIVORCIO POR CAUSAL	1
152 LESIONES, NUM. 2	1
INJURIA	1
DAÑO MORAL	1
ART.75 ENTREGA DEL BIEN O PRESTACIÓN DEL SERVICIO.	1
REQUERIMIENTO JUDICIAL	1
NULIDAD DE INSTRUMENTO PÚBLICO	1
PIRATERIA	1
INCUMPLIMIENTO DE CONTRATO	1
DINERO	1
REINVINDICACIÓN	1
RECUSACIÓN	1
IMPUGNACIÓN CONTRA RESOLUCIÓN DE LAS ADMINISTRACIONES TRIBUTARIAS	1
DEPRECATORIO	1
ACCIÓN DE PROTECCIÓN	1
DIVORCIO POR MUTUO CONSENTIMIENTO	1
INSPECCIÓN JUDICIAL	1
FACTURAS	1
SOLICITUD DE PERITAJE	1
SOLICITUD DE OFICIO	1
DOCUMENTOS	1
INSPECCIÓN PREPARATORIA	1

Fuente: Consejo de la Judicatura

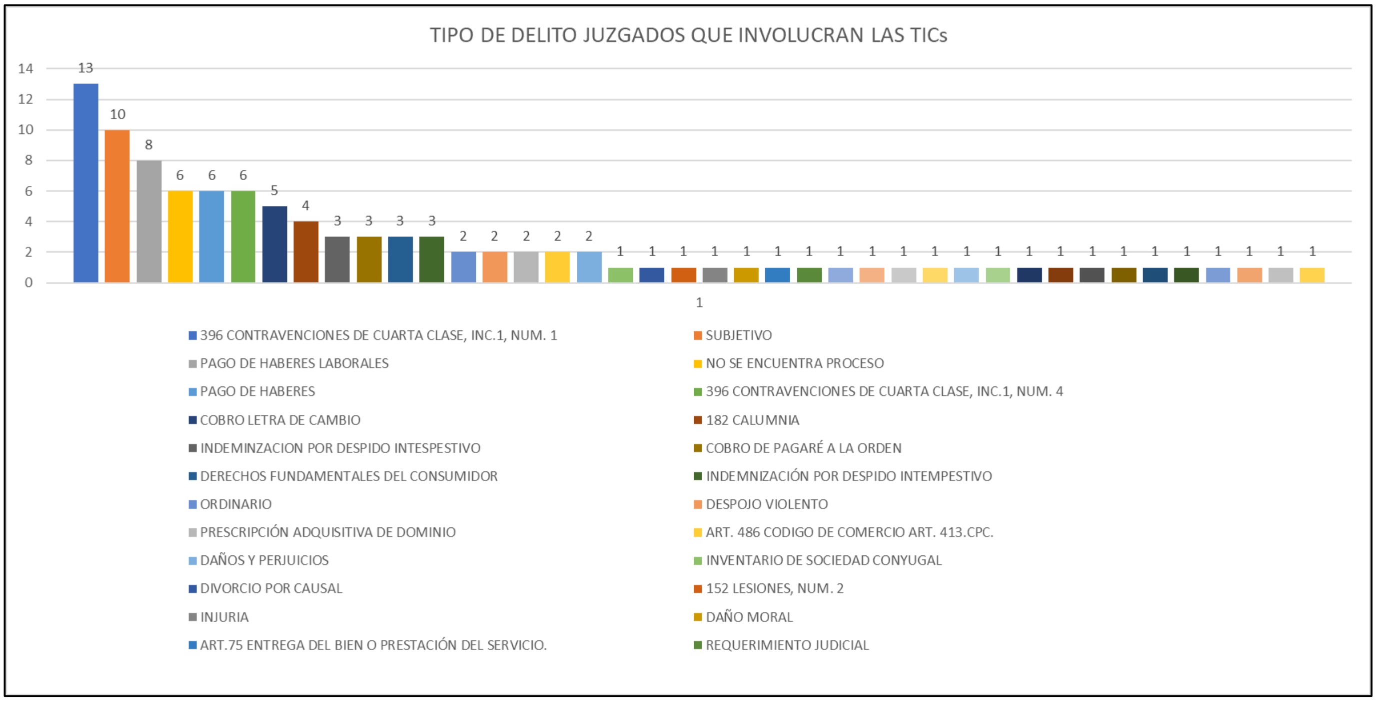


Figura 18: Tipos de Delitos Juzgados que Involucran las TICs con los Informes periciales analizados

En la investigación presentada en el tercer capítulo, se mostraron los artículos del COIP que de acuerdo con los datos de organismos policiales y órganos de justicia son los que más frecuencia usan evidencias digitales para su juzgamiento. El estudio de campo refleja que no solamente en el ámbito penal la evidencia digital es de importancia, sino también en el ámbito civil, laboral y otros como se vio en el análisis de resultados anterior. Se confirma que la Calumnia y la Deshonra a través de redes sociales y otras aplicaciones de internet son las que más presentan evidencias informáticas.

Tabla 22: Delitos juzgados con las pericias informáticas

CAUSA O DELITO JUZGADO	CUENTA	PORCENTAJE
396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 1	13	13%
SUBJETIVO	10	10%
PAGO DE HABERES LABORALES	8	8%
NO SE ENCUENTRA PROCESO	6	6%
PAGO DE HABERES	6	6%
396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 4	6	6%
COBRO LETRA DE CAMBIO	5	5%
182 CALUMNIA	4	4%
INDEMINZACION POR DESPIDO INTESPESTIVO	3	3%

COBRO DE PAGARÉ A LA ORDEN	3	3%
DERECHOS FUNDAMENTALES DEL CONSUMIDOR	3	3%
INDEMNIZACIÓN POR DESPIDO INTEMPESTIVO	3	3%
ORDINARIO	2	2%
DESPOJO VIOLENTO	2	2%
PRESCRIPCIÓN ADQUISITIVA DE DOMINIO	2	2%
ART. 486 CODIGO DE COMERCIO ART. 413.CPC.	2	2%
DAÑOS Y PERJUICIOS	2	2%
OTROS	23	22.33%

Del estudio de campo se determina que el tipo de delito juzgado en el que más intervienen las TICs es “DESHONRA 396 CONTRAVENCIONES DE CUARTA CLASE, INC.1, NUM. 1” con un 12.63%, seguido del tipo de delito denominado como “SUBJETIVO” con un 9.708% y en tercer lugar está “CALUMNIA” con un 7.77%.

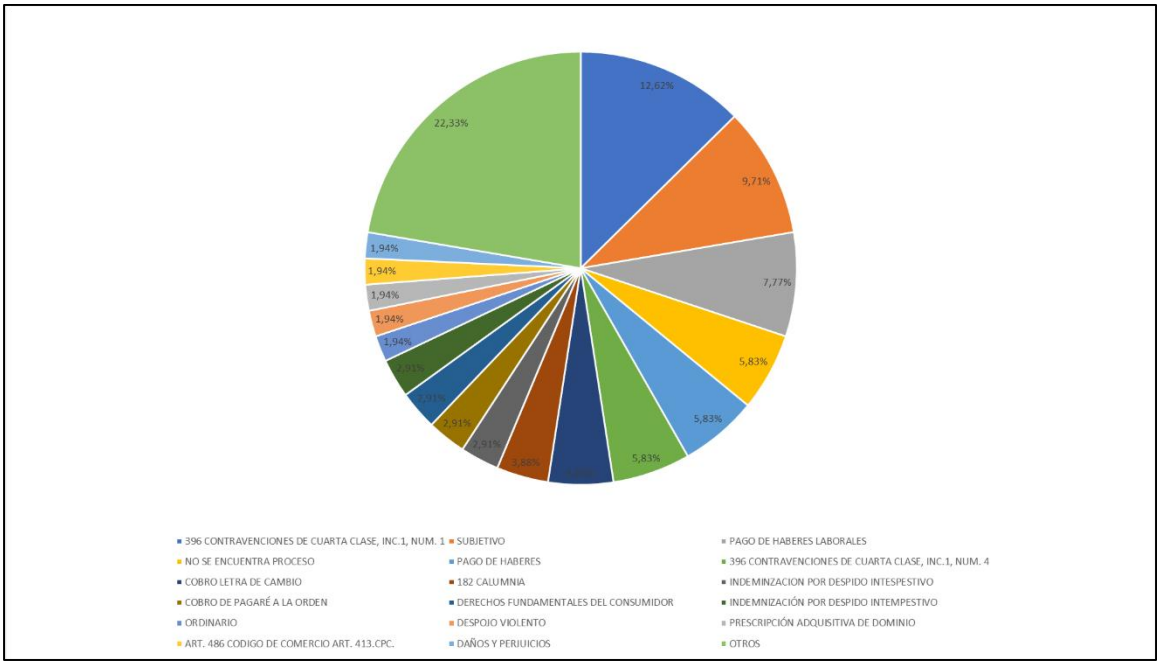


Figura 19: Causas analizadas en los informes periciales

Metodologías, técnicas o métodos forenses aplicados por los Peritos informáticos

Al tratar de identificar si los Peritos han mostrado en los reportes el uso de alguna metodología forense para análisis de las evidencias, se encuentra que 87 de los 103 informes no utilizan una metodología forense.

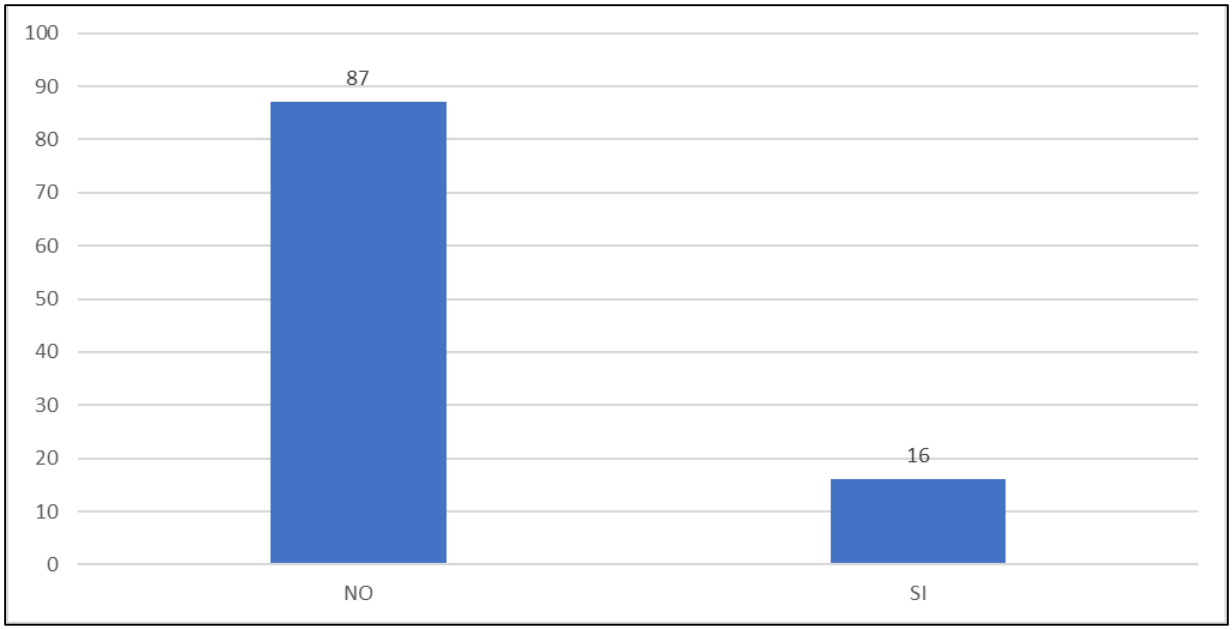


Figura 20: Metodologías, técnicas o métodos forenses aplicados por los Peritos informáticos

El 84.4% de los informes periciales es decir 87 peritos no utiliza una metodología estandarizada o técnica forense para manejo de las evidencias y análisis de estas. Es decir, solo aplican metodologías, procedimientos o técnicas referentes al asunto científico del tema que están informando según su experticia durante el proceso de análisis, cumpliendo con lo que soliciten los abogados de las partes procesales o lo disponga el Juez, limitándose a cumplir con el formato preestablecido para la entrega de informes propuesto por el Consejo de la Judicatura y sin aplicar técnicas o métodos de análisis forense.

Del análisis a las metodologías utilizadas por los Peritos y presentadas en los informes se verifica que empíricamente casi todos cumplen el proceso natural y lógico que comprende las etapas de: recolección de evidencias, el análisis de la evidencia y elaboración del reporte o informe sobre lo analizado.

En la figura 21 se describe las etapas de lo que empíricamente hacen los Peritos, de acuerdo con lo reflejado en sus informes, esto es: Recolección, Análisis e Informe.

Figura 21: Etapas sugeridas por el CJ Ecuador

Al buscar una posible causa a que tan alto porcentaje de profesionales calificados como Peritos informáticos no apliquen técnicas forenses se determina que el proceso de calificación de Peritos

Informáticos del Consejo de la Judicatura no exige a los profesionales una formación forense, ni la escuela de la Función Judicial les dicta capacitaciones en estos contenidos para normar el trabajo de estos y garantizar que se cumpla con los procesos que exige esta actividad.

Como se ha confirmado es necesario que el sistema judicial ecuatoriano norme el análisis forense que realizan los Peritos informáticos calificados por el Consejo de la Judicatura en lo referente al uso de las evidencia y pruebas digitales

Además, la inexistencia de una metodología que guíe su accionar del análisis forense, hace que cada Perito muestre sus conocimientos profesionales sin preocuparse del adecuado manejo de la evidencia; lo que puede afectar a la prueba que constituye el informe pericial. De allí la importancia de que en este trabajo se deje una propuesta metodológica que sea usada por el Consejo de la Judicatura para proteger el accionar de la Justicia en el Ecuador.

Fuentes de la evidencia para las pericias informáticas

Analizando el tipo de evidencias que deben informar los Peritos acreditados al Consejo de la Judicatura, con base en la muestra de informes periciales se determina que en Internet y redes sociales se identifican y recolectan el 36% de las evidencias que se presentan para análisis pericial en procesos judiciales; lo que confirma los índices que se presentaron en el capítulo dos sobre la incidencia del Internet y redes sociales en el cometimiento de delitos. Cuando se trata de conocer cómo se preservan las evidencias casi la mitad de los informes periciales muestran que están en unidades físicas de almacenamiento, siendo las evidencias entregadas en medios físicos la mayor parte con un 45%, la adquisición de evidencias a través de inspecciones a los sitios locales (equipos, sistemas) representan un 19% en la muestra de informes periciales utilizados.

Tabla 23: Fuentes de la evidencia para las pericias informáticas

AMBIENTE DE LA EVIDENCIA	Cuenta	PORCENTAJE
APLICACIÓN INTERNET	20	19%
INSPECCION LOCAL	20	19%
MEDIO FÍSICO	46	45%
RED SOCIAL INTERNET	17	17%
TOTAL	103	100%

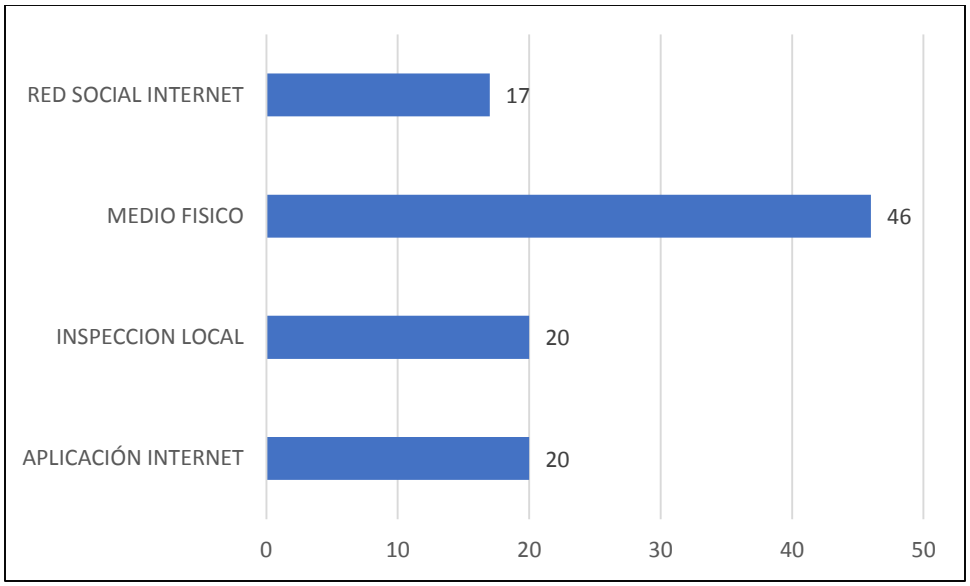


Figura 22: Origen de la evidencia

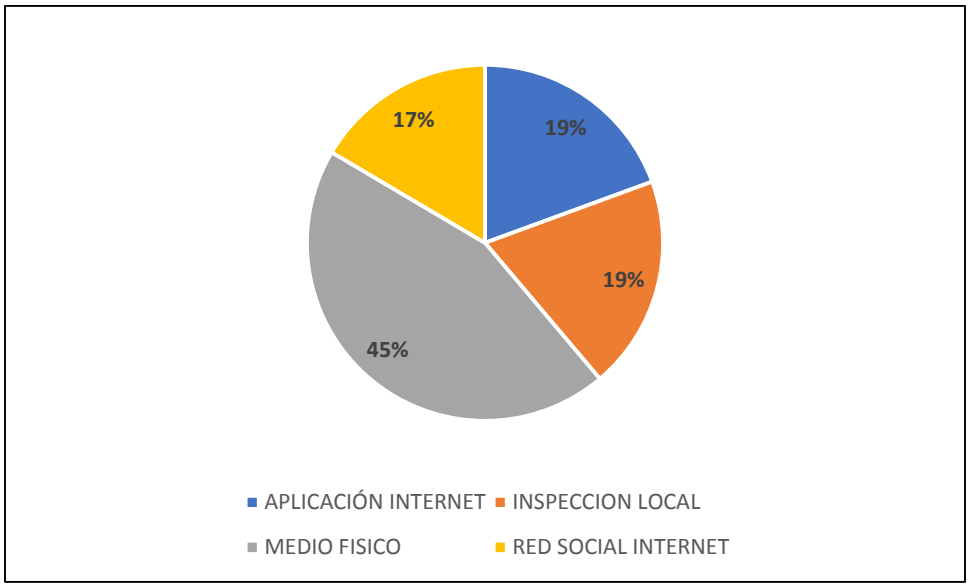


Figura 23: Origen de Evidencias Objeto de Pericias

CAPÍTULO 6: Metodología propuesta

Como se confirmó en el capítulo anterior, el desarrollo de las Tecnologías de la Información y las Comunicaciones (TICs) han evolucionado y permiten que sean cada vez más las personas que poseen acceso a las mismas y por ende las denuncias de delitos incluyen evidencias que involucran TICs. Como se observó en el capítulo tres, la utilización de las TICs trajo ventajas, pero como se describe en los capítulos cuatro y cinco también trajo la aparición de sucesos delictivos mediante el uso de estas. El sistema judicial debe disponer de los elementos para procesar los Juicios con evidencias de esta naturaleza. En el caso del sistema ecuatoriano se ha encargado al departamento de Informática Forense de la Policía Judicial esta actividad la que también es compartida con los Peritos Informáticos calificados por el Consejo dela Judicatura, estos últimos como se ha evidenciado en el desarrollo del capítulo anterior solo un 16% siguen una metodología o procedimientos de análisis forense adecuados y de estos solo el 40% cuentan con las herramientas de informática forense necesarias para una tarea profesional de investigación; por lo que la metodología a proponer va en apoyo a esta actividad de los Peritos del Consejo de la Judicatura más que a los de la Policía Judicial que a saber disponen de laboratorios para cumplir adecuadamente el análisis forense de evidencias informáticas y de telecomunicaciones.

Como se concluye del análisis a los informes periciales entregados por el Consejo de la Judicatura, las causas que más atienden los Peritos informáticos son verificación de mensajes utilizando correos electrónicos, investigación de estafas, calumnias, publicaciones en sitios web, identificación del origen de comentarios calumniosos y de deshonra en redes sociales. El 45% de las pericias se refieren a buscar la extracción y análisis de contenidos de evidencias recopiladas en medios físicos.

La metodología por proponer pretende ser una herramienta que permita guiar a los Peritos en informática en cada una de las etapas de la elaboración de sus análisis de evidencias, de manera tal que pueda ser realizada de forma homogénea y con un procedimiento básico que luego podrá ser adaptado y retroalimentado por el CJ. Esta metodología permitirá contar con un proceso de adquisición legalmente aceptable, apoyado en métodos científicos de recolección, análisis, validación y conservación de evidencias digitales presentadas en las Causas de las Unidades Judiciales del Ecuador.

El planteamiento de una metodología o guía metodológica atiende a requerimientos relacionados con el proceso de obtención y análisis de evidencias digitales necesarios en la elaboración de los informes periciales. Se tomarán como referencia las actividades definidas en el Análisis de Brechas del proceso de computación forense en el Ecuador respecto a las buenas prácticas internacionales (Mera & Benavides, 2018), que brinda una visión del proceso pericial informático en el Ecuador, a partir de las actividades que proponen otras metodologías de análisis forense Informático que abarcan desde la labor de adquisición de evidencias digitales hasta la presentación y manejo de expedientes. Además, para garantizar el cumplimiento de las buenas prácticas para asegurar la

calidad de los procesos aplicados y sus resultados, se considerará como fundamento de la metodología propuesta la familia de normas ISO/IEC 27000, específicamente:

- ISO/IEC 27042:2015 “Guidelines for the analysis and interpretation of digital evidence” (ISO/IEC, 2015), que propone definiciones relacionadas a la evidencia digital.

- ISO/IEC 27037:2012 “Guidelines for identification, collection, acquisition and preservation of digital evidence” (ISO/IEC, 2012), que establece tres principios fundamentales que definen la formalidad de una investigación y son condiciones necesarias y suficientes para que se recaben, aseguren y preserven elementos probatorios sobre medios digitales: relevancia, confiabilidad y suficiencia.

Según el artículo de la revista digital IT-Insecurity (IT-Security, 2013) “Reflexiones sobre la norma ISO/IEC 27037:2012. Directrices para la identificación, recolección, adquisición y preservación de la evidencia digital” indica que la dificultad para validar el cumplimiento de los principios del estándar ISO radica en que el documento de la norma sólo los describe, pero no especifica vías de acción para llevarlos a cabo, de las que se puedan derivar los mecanismos de validación asociados.

Por el amplio espectro de pericias informáticas solicitadas por las Unidades de Justicia del Ecuador, un Perito informático debe contar con una metodología base y el equipamiento necesario para ejecutar cada fase de esa metodología y cumplir con las actividades y procedimientos para garantizar el cumplimiento del adecuado de la pericia informática.

METODOLOGIA DE INFORMATICA Y ANALISIS FORENSE

Del estudio a las metodologías presentadas en el capítulo cuatro, la metodología propuesta debe incluir al menos las siguientes fases:

1. Identificación.
2. Preservación.
3. Análisis.
4. Presentación.

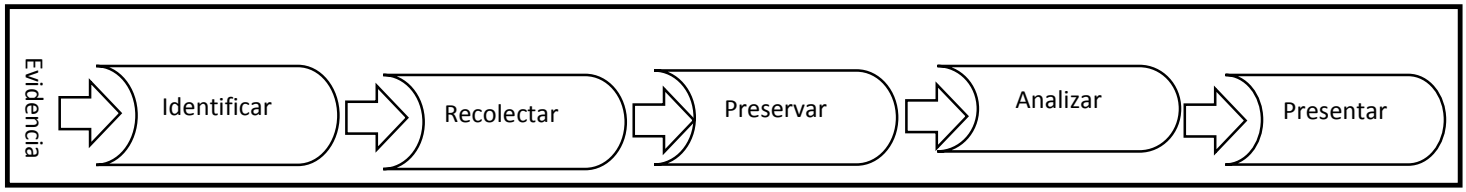


Figura 24: Fases de un análisis forense Digital

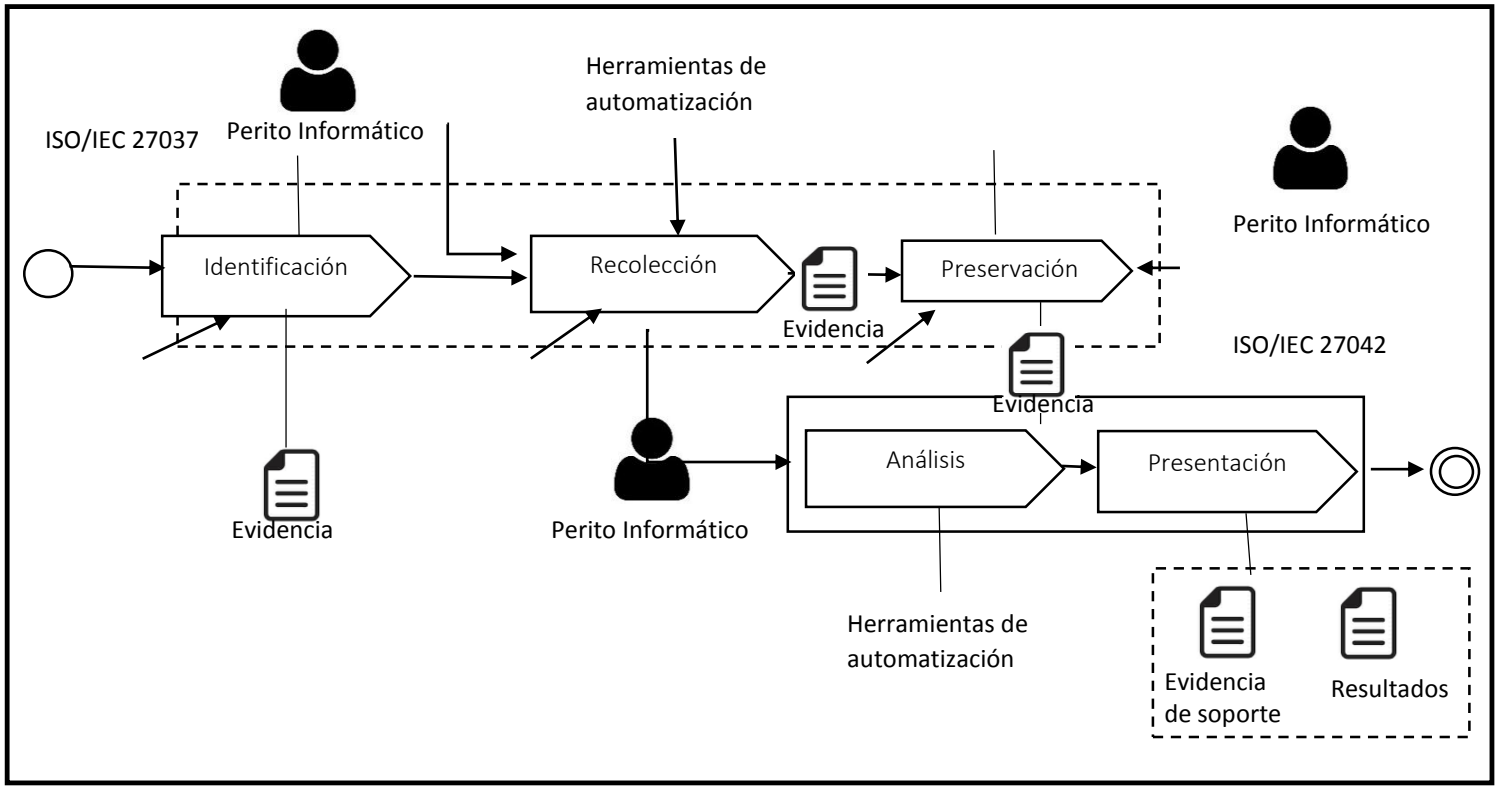
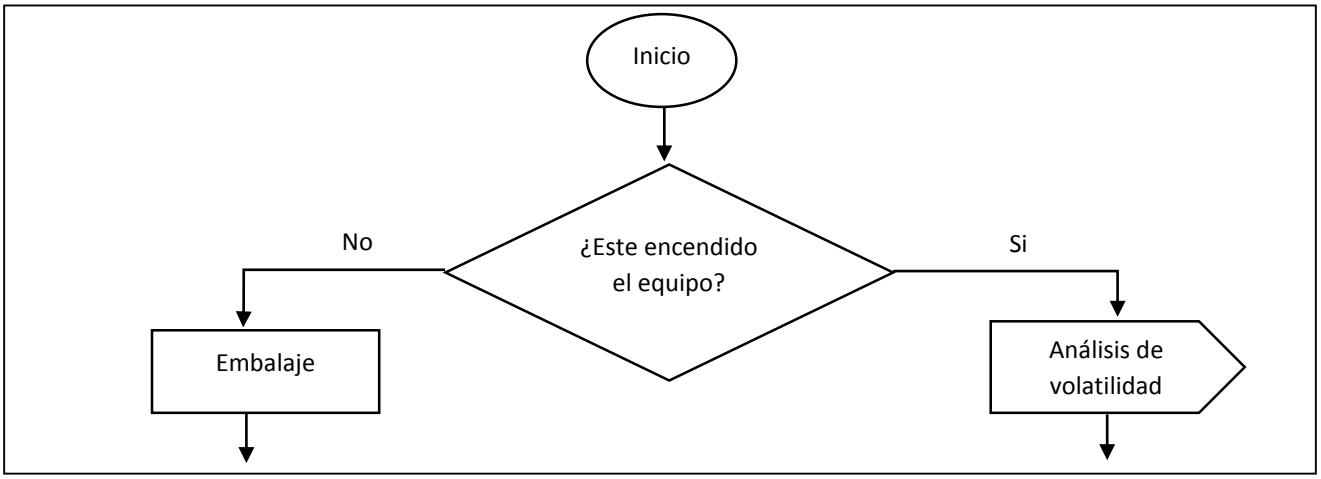


Figura 25: Fases de la metodología propuesta

Además, debe incluir en cada fase o etapa las actividades que se detallan a seguir:

La identificación y Recolección:

Esta fase inicial comprende desde el momento en que el Perito recibe la evidencia o la recolecta y que se muestra a seguir en la figura 26:



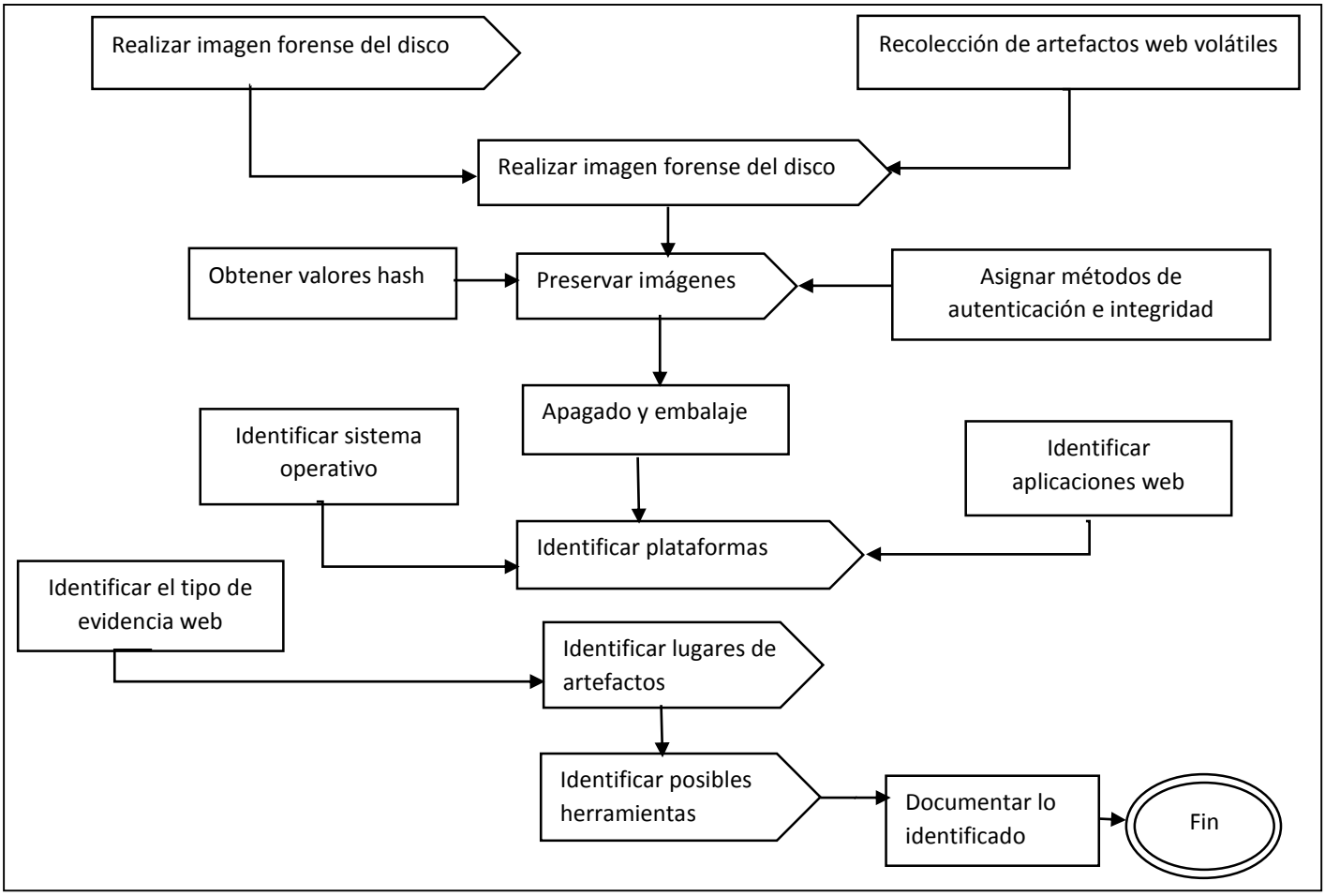


Figura 26: Flujo de tareas y actividades de la fase de identificación

En la figura se distingue que en caso de recolectar la evidencia y si está en funcionamiento o encendida, se debe capturar los procesos que se están ejecutando de ser el caso acorde a la ISO/IEC 27037 (2012). Y realizar el siguiente paso de inmediato para evitar perder información que puede ser de utilidad en la investigación.

Pero en el caso que la evidencia ya este recolectada y embodegada donde un custodio o se encuentre apagada al momento de recolectarla, no se necesita un análisis de volatilidad, simplemente se recomienda retirar el dispositivo de almacenamiento del ordenador y, un correcto embalaje de acuerdo con la ISO/IEC 27037 (2012), luego de esto se puede proceder a realizar la copia bit a bit de la unidad de almacenamiento donde se encuentre la evidencia, realizando una "imagen" del disco, para no alterar la evidencia original y ejecutar la experticia sobre la imagen; posterior hay que generar un proceso para garantizar la integridad de la evidencia (código hash, MD5).

Es importante previo a la recolección y análisis de las evidencias; si la pericia lo requiere identificar los medios físicos o cualquier otro dispositivo, es decir, las diferentes plataformas, aplicaciones

que se utilizaron en el caso; las actividades primordiales de identificación que se recomiendan están: Identificar el sistema operativo, Identificar (de ser posible) que aplicación web es el objeto de la investigación, identificar que navegadores web o aplicaciones de escritorio pudieron ser empleadas; de esta manera se facilita el trabajo para determinar las herramientas apropiadas para la investigación y análisis que desarrolle el Perito (Mahaju y Atkison, 2017; Nalawade, 2016).

En algunas pericias es necesario identificar lugares de artefactos (aparatos, equipos o simplemente cosas) web, Esta actividad se basa en identificar las posibles direcciones IP de los equipos están conectados o direcciones del Sistema Operativo dónde las aplicaciones web almacenan la información que manejan, por ejemplo, archivos temporales o logs de actividades. Esta información puede ser útil para identificar si las herramientas de automatización son efectivas, es decir si las mismas examinan estos lugares, y en el caso de que no existan herramientas que examinen estos lugares, la búsqueda debe ser manual o las herramientas podrían ser creadas por el investigador. Por lo general los lugares en donde se da la interacción con aplicaciones web está en:

- Navegadores: Se debe verificar la ruta en la que el navegador almacena sus artefactos web dependiendo del sistema operativo, los artefactos que se pueden encontrar son: cookies, cachés de navegación, historiales de navegación, historiales de accesos, cuentas, etc.
- Aplicaciones de escritorio: Se verifica el directorio de la aplicación, por lo general las aplicaciones de escritorio utilizan archivos temporales, o generan logs de sus actividades.

En las siguientes figuras se muestran los formatos para identificación de evidencias digitales a examinar usados por el Departamento de Justicia de los Estados unidos y por la Legislación Argentina, estos se completarán por el Perito al momento que reciba o recolecte la evidencia.

DESCRIPCIÓN DE LA EVIDENCIA				
1 tipo = BD – Disco Blu-Ray; Cam Cámara Cd – Disco compacto; INSTALACIONES BÁSICAS Escritorio Dsk Disquete Dvd – Disco de vídeo digital; Dvr – Grabadora de vídeo digital; ExtHDD – disco duro externo; Fax Facsímil Fsm – Medios Flash; Gam – Estación de juegos; Gps – Sistema de posicionamiento global; Hdd – Disco duro; Regazo – PortátilPho – Teléfono; Prn – Printer;Sí – Tarjeta SIM; Srv Servidor pestaña Tableta Grifo – Cintas de backup; Thm – Pulgar Unidades; Proporcione la descripción de cualquier otro dispositivo no enumerado anteriormente (es decir, adaptadores inalámbricos USB, etc.)				
RX RInformes	Aplicación SoftwareVersión (McKesson 6.2.1, etc.)			
Tipo:[1]	Fabricante:	Modelo:	Identificación de tipo y número:	Capacidad
pestaña	Microsoft	Surface Pro MN: 1631	SN: 052782443753	
Hdd		N/A	N/A	256 GB

INFORMACIÓN DE IMÁGENES								
Laptop/TD1/TD2 propiedad # o SN:	N/A				Software y versión: (N/A para TD1/TD2)	FTK Imager 3.4.2.2		
Nombre de la imagen:	HMS020				Tipo de imagen:		físico	X Lógica
Sistema sospechoso usado	X	Sí		No	Write Blocker SN:(N/A si se utiliza como puente solamente)	N/A		
Ubicación de adquisición zona horaria:	UTC-5				* Sistema sospechoso Fecha/hora²:	N/A		
Ubicación de adquisición fecha/hora²:	UTC-5				* Explique a continuación si no se puede obtener.			
2 formato de fecha/hora = MM-DD-yyyyhh: mm (Puede entrar sin colon, guión y espacio.)								

INFORMACIÓN DE VERIFICACIÓN DE IMAGEN						
Laptop/TD1/TD2 propiedad # o SN:		Verificado:		Hash		Estructura de archivo
Software y versión: (N/A para TD1/TD2)						

Comania Doremetals, S.a
Ubicación de imágenes (SFL9 o ubicación de OSB si es diferente de la ubicación de la orden): Pev
Información de usuario (Nombre de usuario, posición, contraseñas, etc.) Sólo para uso de OSB: Contraseña encontrada en el teclado de Surface-"andrea10". Nombre de usuario "Elias Quiero"

Notas:

Dispositivo móvil: [Symbol]N/A

Tipo:	Smartphone	**Número de teléfono:**	N/A
Fabricante:	Samsung	**Nombre del modelo/no.:**	SM-G313ML
Identificador único:	SN: R21G323KN9X		
Proveedor de servicios:	Claro	**Capacidad**:	4 gb
Funcionalidad:	N/A	**Tipo de sistema operativo y versión no.:**	Android 4.4.2
Información del usuario:	N/A		
Zona horaria del dispositivo:	UTC-5	**Zona horaria real:**	UTC-5

Estado de bloqueo de dispositivo óvil:

La exhibición fue bloqueada tras la inspección inicial:	[Symbol] Sí	[Symbol] No	[Symbol] N/A
Fue el valor de desbloqueo proporcionado por la oficina de solicitud:	[Symbol] Sí	[Symbol] No	[Symbol] N/A
¿Pudo determinar el valor de desbloqueo durante el examen Proceso:	[Symbol] Sí	[Symbol] No	[Symbol] N/A
Valor de desbloqueo:	N/A		

Tarjeta SIM: [Symbol]N/A

Número de teléfono:	N/A	**Proveedor de servicios:**	N/A
ICCID	89530100059263504	**Bloqueado:**	[Symbol]Sí[Symbol]No

Tarjeta de medios:	[Symbol]N/A		
Fabricante:		**Modelo:**	N/A
Identificador único:		**Capacidad:**	

Notas:

Tabla 24: Número de delitos registrados en el periodo 2017-2019

NOTICIAS DE DELITOS	AÑO 2017	AÑO 2018	ENERO 2019
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	220	241	19
Apropiación fraudulenta por medios electrónicos	958	1430	168
Ataque a la integridad de sistemas informáticos	86	88	6
Comercialización ilícita de terminales móviles	24	13	
Delitos contra la información pública reservada legalmente	14	12	
Espionaje	1	1	
Interceptación ilegal de datos	63	41	5
Pornografía con utilización de niñas, niños o adolescentes	107	105	11
Reemplazo de identificación de terminales móviles	5	2	
Reprogramación o modificación de información de equipos terminales móviles	7	4	1
Revelación de secreto (Por parte de profesional que debe guardar reserva)	13	13	2
Revelación ilegal de base de datos	21	45	2
Suplantación de identidad	3672	4177	450
Supresión, alteración o suposición de la identidad y estado civil	52	81	11
Terrorismo	13	90	6
Transferencia Electrónica de activo patrimonial	59	37	3
Violación a la intimidad	1651	2065	204
TOTAL	6966	8445	888

Fuente: Fiscalía General del Estado

Tabla 25: Ejemplo de registro de incidencias de la LOPD

Apropiación fraudulenta por medios electrónicos	958	1430	168
Ataque a la integridad de sistemas informáticos	86	88	6
Comercialización ilícita de terminales móviles	24	13	
Delitos contra la información pública reservada legalmente	14	12	
Espionaje	1	1	
Interceptación ilegal de datos	63	41	5
Pornografía con utilización de niñas, niños o adolescentes	107	105	11
Reemplazo de identificación de terminales móviles	5	2	
Reprogramación o modificación de información de equipos terminales móviles	7	4	1
Revelación de secreto (Por parte de profesional que debe guardar reserva)	13	13	2

Revelación ilegal de base de datos	21	45	2
Suplantación de identidad	3672	4177	450
Supresión, alteración o suposición de la identidad y estado civil	52	81	11
Terrorismo	13	90	6
Transferencia Electrónica de activo patrimonial	59	37	3
Violación a la intimidad	1651	2065	204
TOTAL	6966	8445	888

Fuente: Fiscalía General del Estado

En el caso de los delitos que se cometen a través de TICs, de las pericias presentadas en los informes del capítulo cinco, se desprende que es menor la recolección de evidencias por parte del Perito, la mayoría de las evidencias son entregadas de manera directa por los actores, por lo que la identificación es una actividad importante que casi no se cumple.

La Figura 27 muestra las tareas y actividades de la fase de recolección que debería realizar el Perito informático.

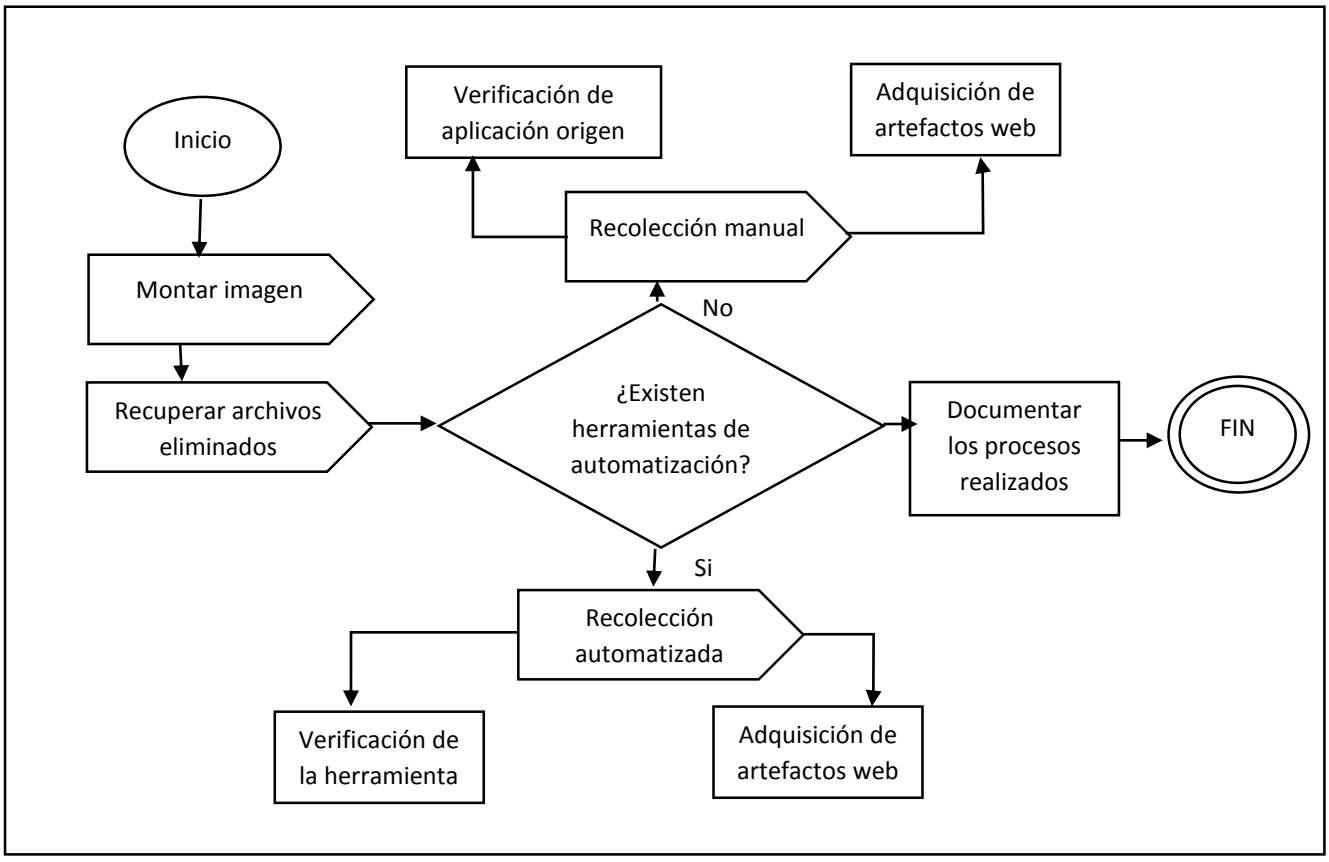


Figura 27: Tareas y actividades a desarrollarse en la fase de recolección

Según la recomendación de la ISO/IEC 27037 y 27042 se debe bloquear cualquier tipo de escritura en la evidencia, por lo que esta actividad debe previamente hacerse la verificación de que la

evidencia con la que se trabaja es integra a través de la comprobación de códigos hash, firma digital u otro método usado. Si fuese el caso, en esta actividad se recuperarán archivos eliminados, ocultos, borrados.

Generalmente, se emplean herramientas que automatizan este proceso, pero en caso de no existir una herramienta, ya sea por la dependencia del sistema operativo o la dependencia de las aplicaciones; el Perito debe realizar una recolección manual de las evidencias que pudieron ser dejados por la aplicación Web. Es conveniente asegurarse que los logs, archivos temporales, archivos que la aplicación utilizó sean recolectados. En caso de que la aplicación que se utilizó para la interacción hubiera sido un navegador (Explorer, Google Chrome), también se debe asegurar que se recolecto el historial, registros de favoritos, historiales de descargas, caché y cookies del navegador. De no encontrar mayores artefactos web, es posible que se haya utilizado una sesión privada o portable, en tales casos la información que se conserve será menor, por lo que se sugiere analizar los archivos de las extensiones de los navegadores pues las mismas no poseen modo incógnito o acudir a la memoria RAM. La norma ISO/IEC 27037 (2012) sugiere identificar las carpetas, archivos o cualquier opción de sistema propietario relevantes para adquirir los datos deseados, para luego realizar la adquisición lógica de esos datos identificados. O también es recomendable investigar y emplear técnicas de minería de datos (Miranda López, 2016). Al finalizar las actividades de esta fase las salidas serían las siguientes:

- Documentación de la evidencia web recolectada, su procedencia y el tipo de esta.
- Evidencia digital recolectada.

Otras actividades que el Perito debe tener en cuenta en esta fase son:

- Determinar qué proceso adicional puede ser necesario continuar la búsqueda si llegase a encontrar una evidencia que no estaba autorizada en la orden del Juez o Fiscal (Departamento de Justicia de Estados Unidos).
- Supervisar la cadena de custodia previa hasta la llegada de las evidencias al entorno de análisis forense (Argentina).
- Preparar un plan de investigación documentada que ayude a la determinación de los recursos, la selección de los procesos y herramientas para orientar al equipo de investigación (ISO IEC 27043).
- Realizar una labor previa de localización de las evidencias que confirme la existencia de un incidente y las causas que lo originaron (Argentina).
- Validar y confirmar los procesos que implican el uso de nuevos instrumentos antes de la implementación (ISO IEC 27042).
- Tener un kit de herramientas forenses para la recolección de datos, examen y análisis (Instituto Nacional de Estándares y Tecnologías España).
- Conocer el objetivo, alcance y destinatarios que tendrá la investigación (ISO IEC 27042).
- Incluir un documento de recepción y registro de la evidencia recibida (Argentina).

- Redactar el detalle de las informaciones recibidas y las decisiones que se toman, incluidos los motivos de la decisión (ISO IEC 27042).
- Documentar cada paso ejecutado en la adquisición de los datos (España).
- Determinar los posibles tipos de pruebas que se persiguen (Departamento de Justicia de Estados Unidos).
- Adoptar los principios de la cadena de custodia al soporte de la información adquirida, acompañada de la obtención de un código hash para posterior validación (Argentina).
- Crear un acta de levantamiento de evidencia digital (Argentina).
- Localizar todos los equipos inalámbricos determinando todos los modos de comunicación que usan éstos (Argentina).
- Documentar el estado del dispositivo como marca, modelo, tamaño, configuración, ubicación, MAC, tarjeta de red entre otros que se consideren fundamentales. (Departamento de Justicia de Estados Unidos).
- Fotografiar y etiquetar las pruebas para proporcionar recordatorios visuales de la configuración del equipos y periféricos (Argentina).
- Desconectar los dispositivos de almacenamiento para evitar la destrucción, deterioro o alteración de los datos. (Departamento de Justicia de Estados Unidos).
- Si se detecta que el dispositivo está accediendo a datos remotos, archivos encriptados o con claves de acceso, correspondencia o comunicaciones electrónicas, datos de carácter personal entre otros se debe consultar al responsable del procedimiento acerca de los límites que pudieran existir para la captura de la información (Argentina).
- Hacer uso de herramientas de adquisición de datos confiables (España).
- Realizar dos resúmenes digitales (hash) de la información contenida en el disco duro de forma simultánea al proceso de clonado, usando herramientas de hardware o software contrastadas en el ámbito forense y verificar que ambos resúmenes sean los mismos. UNE 71506:2013.
- Procurar la menor alteración y /o destrucción de datos informáticos; de darse el caso debe precisar en forma documentada en que ha consistido la alteración y cuáles son los efectos sobre el material probatorio adquirido. (Guía Integral Argentina).
- Ejecutar el levantamiento de los datos acorde al previo análisis de niveles de relevancia o prioridad, del tipo de dispositivo y del orden de volatilidad de la información. (Guía Integral Argentina).
- Verificar la integridad de los datos adquiridos (Instituto Nacional de Estándares y Tecnología).
- Discutir si otros procesos forenses tienen que llevarse a cabo sobre la evidencia (Departamento de Justicia de Estados Unidos).
- Analizar la posibilidad de emprender otras vías de investigación para obtener más pruebas digitales (Departamento de Justicia de Estados Unidos).
- Determinar información adicional que puede ayudar a resolver el caso (Departamento de Justicia de Estados Unidos).

Preservación

Esta fase muchas veces se da en simultaneo con la identificación, al momento de almacenar en discos "imagen" digitales, es recomendable garantizar que solo las personas que deben tengan acceso a la misma, por lo que se sugiere utilizar métodos de autenticación e integridad (como: firma digital, valores hash, claves primarias).

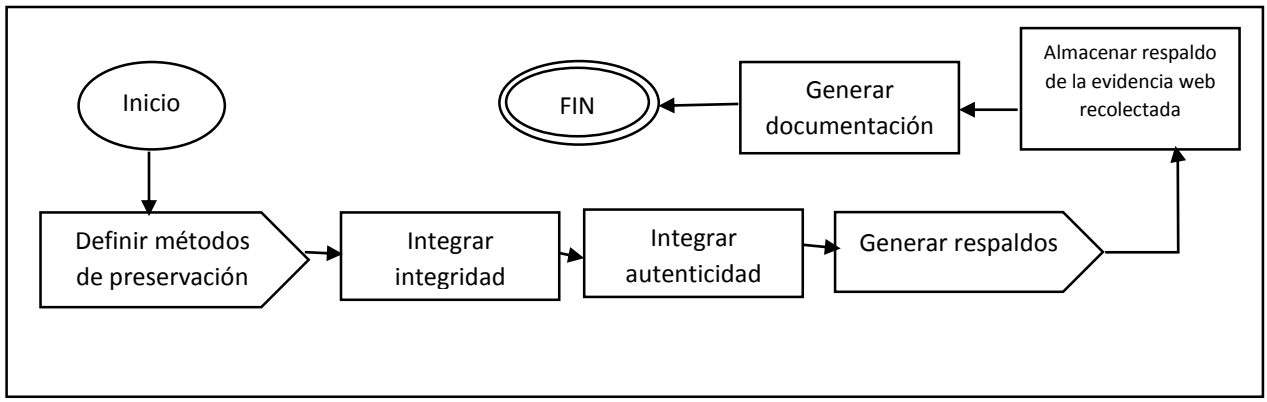


Figura 28: Tareas y actividades de la fase de preservación

Al iniciar esta fase es necesario que la entrada de esta sea la evidencia recolectada, en la figura 28 se muestran el flujo de tareas y actividades de esta fase (Coronel, 2018). Por lo general los métodos de preservación son definidos y seleccionados por el Perito.

Los métodos de preservación son necesarios para garantizar autenticación e integridad sobre la evidencia recolectada. Para cumplir con estas características obligatorias en una investigación forense se puede utilizar claves de acceso, verificaciones de sumas (checksums), firmas digitales o valores hash (Lee, 2005).

Se debe utilizar una función de verificación, para proveer evidencia de tal forma que las copias sean idénticas a la original. Además, es recomendable asociar la evidencia con el Perito manipulando formatos digitales con fotografía y firma de acuerdo con la recomendación ISO/IEC 27037 (2012).

También es recomendable mantener la evidencia que se ha recolectado respaldada y preservada, para que si existe alguna alteración de la evidencia con la que se está trabajando se pueda recurrir al respaldo. El respaldo debe mantener una identificación del dispositivo de almacenamiento. Además, es importante mantener la cadena de custodia en archivos personales del Perito o del juzgado.

De las metodologías internacionales (USA, España, Argentina) se puede incluir en esta etapa o fase las siguientes actividades:

- Impedir el acceso no autorizado y la alteración de las pruebas.

- Designar a una persona como custodio de pruebas, donde tenga la responsabilidad exclusiva de fotografiar, documentar y etiquetar cada elemento que se recoge, y registrar cada acción Instituto Nacional de Estándares y Tecnología que se realizó junto con quien realiza la acción, dónde fue realizado y en qué momento.
- Fotografiar y grabar en video la escena de interés (España).
- Manipular las evidencias con la indumentaria adecuada, especialmente adaptada para evitar descargas electrostáticas. (España).
- Efectuar un estudio del área física y reconocer las posibles fuentes de datos (Argentina).
- Determinar el número y tipo de equipos en la escena (Departamento de Justicia de Estados Unidos).
- Documentar la ubicación desde el cual los medios fueron retirados. (Departamento de Justicia de Estados Unidos).
- Aislar los sistemas pertinentes de influencias externas para prevenir mayores daños al sistema. (Argentina).
- Documentar los detalles de cada una de las pruebas encontradas antes y durante el proceso de análisis forense (Departamento de Justicia de Estados Unidos).
- Crear una lista de todos los usuarios que tienen acceso a los equipos que están siendo analizados para que puedan proporcionar sobre el lugar de alguna información importante. (Argentina).
- Evaluar la necesidad de proporcionar alimentación eléctrica continua para aparatos que funcionan con pilas. (Departamento de Justicia de Estados Unidos).
- Almacenar la evidencia digital en soportes adecuados antes y durante el análisis para garantizar la integridad (USA).
- Embalar y sellar en soportes adecuados todas las evidencias encontradas, hasta que se active su análisis por los Peritos dentro del laboratorio de análisis forense para garantizar la integridad. (USA).

Análisis

Esta fase se inicia al recibir la evidencia preservada, en la mayoría de los informes periciales. El objeto de estos se orienta al cumplimiento de esta fase, es entonces la fase más importante del Perito, por lo que debe documentar como encontró o recibió la evidencia. Previo a iniciar el Perito debe verificar que la evidencia esté integra a través de cualquier proceso de autenticación, en el detalle de las actividades de esta etapa se exponen algunos de estos métodos.

A pesar de que se utilicen herramientas tecnológicas forenses para el Análisis, la interpretación de los resultados en los reportes de estas herramientas debe ser hechos por el Perito en apoyo a la investigación y ese ejercicio intelectual se da en esta fase.

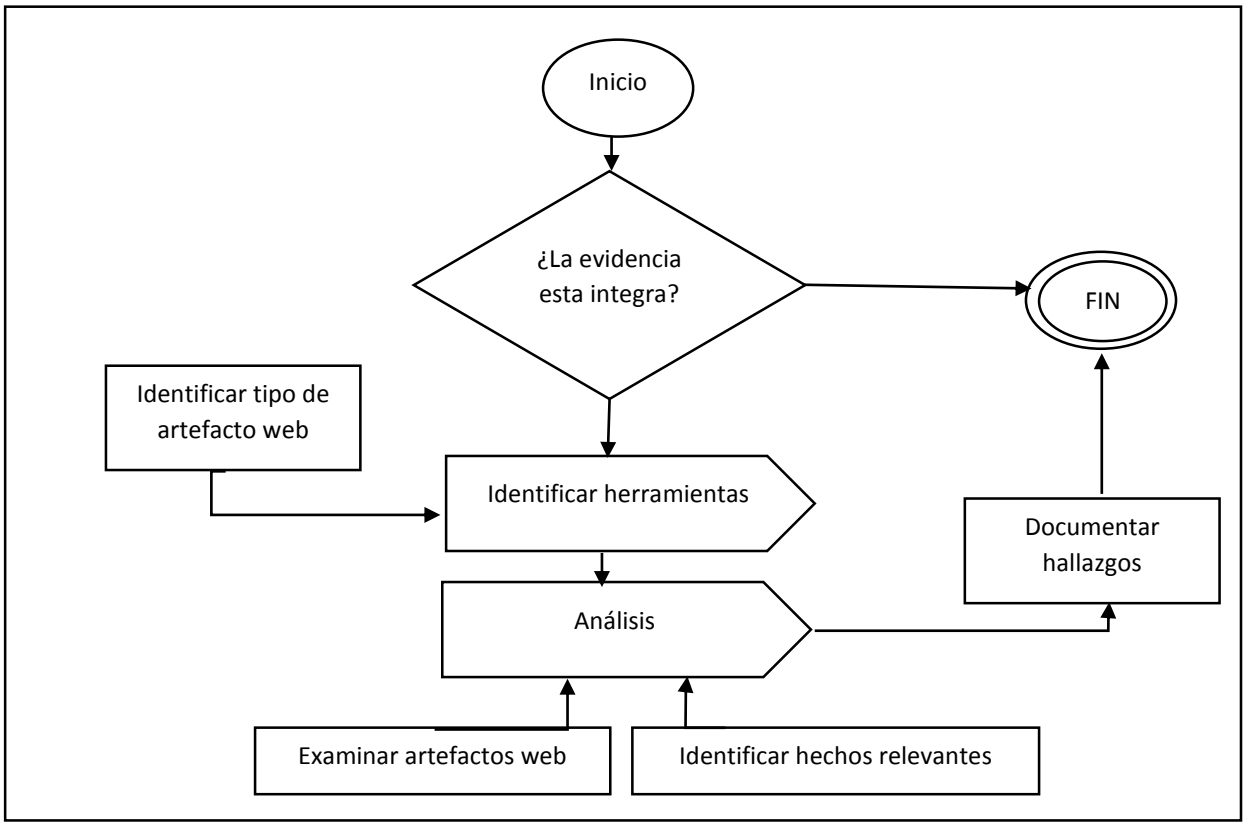


Figura 29: Tareas y actividades en la fase de análisis

En el caso de los informes periciales no se aprecia análisis forenses, a parecer los incidentes a redes o sistemas informáticos en el Ecuador no son reportados ni registrados por el Estado, actividad que merece un estudio futuro.

La etapa de análisis incluye:

Estudio preliminar. En esta fase se realiza un estudio inicial mediante entrevistas y documentación entregada por el Abogado, Juez o Fiscal; con el objetivo de tener una idea inicial del problema que se va a tratar.

Se realiza una obtención de los datos e informaciones esenciales para la investigación. Se duplican o respaldan los dispositivos implicados que se van a analizar a través de discos “imagen”. En esta fase habrá que tener mucho cuidado en la adquisición de los datos puesto que cabe la posibilidad de incumplir los derechos del demandado.

Se realiza un estudio con los datos adquiridos en la fase anterior. En esta actividad también habrá que tener mucho cuidado puesto que cabe la posibilidad de incumplir los derechos fundamentales del actor o demandado.

Actividades que recomiendan las diversas metodologías estudiadas, que deben ejecutarse durante el análisis son:

- Establecer el orden de prioridad de la prueba que se va a examinar Departamento de Justicia de Estados Unidos.
- Mantener notas contemporáneas detalladas y precisas de las cada actuación ejecutada y los procesos que estas demandaron. ISO IEC 27042
- Comprobar que las evidencias no están deterioradas y son susceptibles de su estudio forense UNE 71506:2013.
- Identificar los tipos de archivos desconocidos para determinar su valor en la investigación Departamento de Justicia de Estados Unidos.
- Revisar los encabezados de los archivos Instituto Nacional de Estándares y Tecnología.
- Especificar la hora de la BIOS del equipo informático en donde van instalados los discos duros que contienen la información de interés UNE 71506:2013.
- Revisar los registros del sistema y de las aplicaciones que puedan estar presentes como registros de error, registros de instalación, conexión de registros, registros de seguridad entre otros. Departamento de Justicia de Estados Unidos
- Revisar los sellos de fechas y hora que figura en el sistema de archivos de metadatos para vincular archivos de interés. Departamento de Justicia de Estados Unidos.
- Examinar la estructura de partición del disco para determinar si todo el tamaño físico de la unidad de disco duro se contabiliza. Departamento de Justicia de Estados Unidos.
- Revisar nombres de archivos relevantes y patrones Departamento de Justicia de Estados Unidos.
- Examinar las relaciones entre archivos Departamento de Justicia de Estados Unidos.
- Estudiar la documentación adjunta a las evidencias UNE 71506:2013.
- Considerar nuevas evidencias relevantes en el proceso que no habían sido contempladas en un principio, iniciando nuevamente la reseña de éstas, generando un nuevo proceso de gestión, custodia y trazabilidad. UNE 71506:2013.
- Informar a quien solicitó el peritaje si se encuentra nuevas evidencias del incidente y esperar por nuevas instrucciones ISO IEC 27042.

Informe o reporte

Una vez que se han cumplido las etapas anteriores, en esta fase el Perito informático documentará toda la información que generó en las etapas previas, resaltando la información de relevancia para la toma de decisiones del Juzgador o interesado en el caso investigado. Se recomienda detallar una línea de tiempo de los eventos que sucedieron con la evidencia y registrarlos en esta fase sustentándolos con los procesos que desarrollo el Perito en cada evento.

El informe debe ser redactado de forma que sea fácil de entender para personas no técnicas en lo posible, pero debe contener el sustento que apoye los resultados obtenidos.

Es importante conocer que todos los resultados obtenidos deben poder ser utilizados por otros investigadores según la ISO/IEC 27037 (2012).

En este reporte, la evidencia preservada debe ser adjuntada. Se debe asegurar que cuando la evidencia va a ser presentada esta contenga métodos para permitir únicamente la lectura de esta y no permitir modificaciones. Según la ISO/IEC 27037 (2012) en el reporte emitido por el Perito se debe considerar:

1. Ningún detalle sea dejado fuera durante el proceso de identificación, recolección adquisición y preservación de la evidencia.
2. El investigador debe considerar que el tiempo de los equipos, si están encendidos los mismos, este sincronizados con la hora válida, de ser posible comparar con una fuente de tiempo confiable y registrar aquello en el informe.
3. Registrar todo lo visible por el monitor o pantalla del dispositivo; pudiendo ser programas activos, procesos, nombres de documentos abiertos. Estas capturas deben registrarse con una breve descripción.
4. Cualquier movimiento con el ordenador debe ser registrado en la documentación.

En el caso del estudio de campo se verifica que todos por Peritos cumplen esta fase, de acuerdo con la estructura que dispone el CJ que comprende:

1. Antecedentes
2. Consideraciones técnicas y metodologías aplicadas
3. Conclusiones
4. Anexos

Actividades que deben tenerse en cuenta en la elaboración del Informe son:

- Ubicar la identidad de la agencia/departamento/unidad y Perito(s) que ejecutaron el análisis forense. (Departamento de Justicia de Estados Unidos)
- Ubicar el número identificador del caso, la fecha de recepción del caso y la fecha del informe (Departamento de Justicia de Estados Unidos)
- Incluir la naturaleza de los hechos investigados, la ubicación donde ocurrió la incidencia, el objetivo de la investigación, los miembros del equipo de investigación junto a sus funciones, la duración de la investigación, la ubicación de la investigación, los detalles de las pruebas digitales que se han observado durante la investigación. (ISO IEC 27042)
- Incluir una declaración clara del escritor que participó en la investigación. (ISO IEC 27042)
- Usar una plantilla de informe con formato estandarizado para ayudar a garantizar que existe suficiente información incluida en los mismos. (ISO IEC 27042)
- Detallar la información general de los dispositivos analizados, tales como marca, modelo, número de serie entre otros. (Departamento de Justicia de Estados Unidos)

- Describir brevemente las medidas adoptadas durante el examen, tales como búsquedas de cadenas, búsquedas de imágenes, gráficos y recuperar archivos borrados Departamento de USA
- Describir los programas utilizados en el análisis de la evidencia (Departamento de Justicia de Estados Unidos)
- Detallar las técnicas utilizadas (Departamento de Justicia de Estados Unidos)
- Informar si las pruebas digitales han tenido cualquier daño (ISO IEC 27042)
- Determinar los resultados y conclusiones del caso. (Departamento de Justicia de Estados Unidos)
- Incluir las limitaciones de cualquier análisis realizado (ISO IEC 27042)
- Incluir las recomendaciones para continuar con la investigación o trabajos futuros. (ISO IEC 27042)

Al culminar esta fase se debe obtener el Informe Pericial con sus Anexo y Apéndice, Anexos obligados son las evidencias, documentos, archivos, etc. de sustento de todo lo informado

En el anexo B, se puede encontrar un informe pericial en el formato dispuesto por el CJ

Propuesta de herramientas tecnológicas

Para cumplir con la multiplicidad de pedidos de pericias que llegan a los Peritos desde las Unidades Judiciales (Juzgados), y en los de profesionalizar su actividad de ayudante de justicia, se recomienda que un Perito debe tener acceso a disponer como elementos de trabajo específicos algunas herramientas tecnológicas con las debidas capacitaciones y certificaciones en lo posible. Esta propuesta se hace con la intensión de suplir las necesidades más esenciales basadas en las estadísticas de los tipos de pericias solicitadas y analizadas en el capítulo cinco y con base en las herramientas propuestas en el capítulo cuatro.

a. Bloqueador de Escritura: una herramienta de hardware que permite la conexión de diferentes dispositivos de almacenamiento (IDE/SATA) bloqueando el mismo ante escrituras. Esto permite de forma segura, evitando la escritura sobre los medios conectados, un análisis rápido de los archivos existentes. En particular se eligió el Tableau T35es-R2 por los siguientes motivos:
    - Brinda una solución integral que nos permite comprender los datos.
    - Existen actualizaciones periódicas, es decir, las funcionalidades necesarias están disponibles.
    - Es más que un software, brinda capacitación para la organización, en este caso los peritos.
b. Evidencia de Comunicaciones en Internet: es un producto de software que obtiene los rastros de navegación, chats de diferentes proveedores de servicios (skype, facebook, etc), actividad de envío y recepción de emails, etc. Permite visualizar, recuperar y analizar comunicaciones basadas en el protocolo de Internet. En este caso se optó por el Internet Evidence Finder. Dado que:

- Analiza cientos de artefactos de computadoras y dispositivos móviles que le permiten encontrar rápidamente la información relevante.
- Recupera evidencia de archivos que se encuentran en espacios no localizados.
- Visualizar evidencia digital en una secuencia organizada y cronológica.

c. Búsquedas por Patrones: en muchas ocasiones es necesario buscar información en una imagen forense de un dispositivo de almacenamiento completo en los cuales EnCase Forensic y/o AccessData FTK pueden ser aliados en nuestras investigaciones. Aquí es necesario adquirir el equipamiento asociado dado que ya no se podrá usar una simple PC de escritorio, sino que se necesitará una plataforma avanzada y potente que el mismo fabricante de software ayuda a configurar, convirtiéndose en una verdadera estación de trabajo forense.

Si se requiere tener una infraestructura dedicada a la adquisición y preservación automatizada de evidencias digitales, autores como Hernán Herrera y Leopoldo Gómez (Herrera & Leopoldo, 2018) proponen una solución informática extensible para laboratorios de informática forense que facilite el análisis de dichas evidencias a través de la gestión automatizada y el monitoreo de un conjunto de tareas vinculadas con el procesamiento de datos en el marco de una pericia informática.

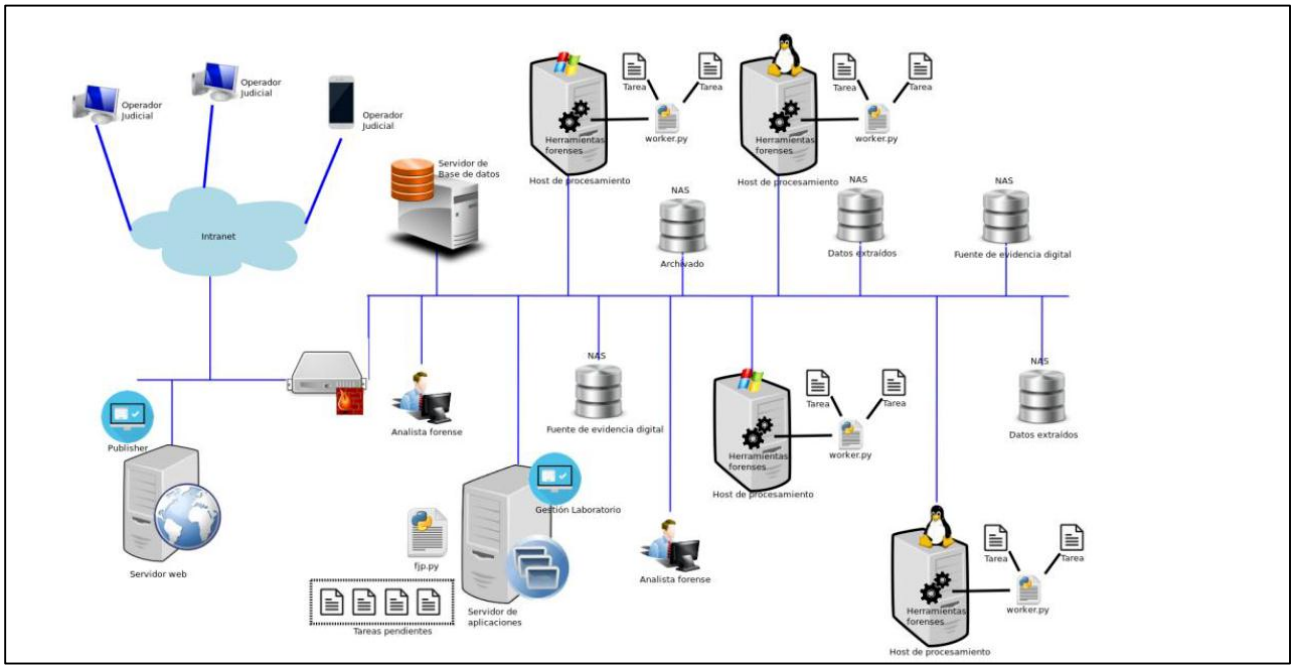


Figura 30: Arquitectura para la gestión automatizada de actividades operativas.
Fuente: Poder Judicial de Neuquén

La aplicación funciona sobre una infraestructura compuesta por una red local de alta velocidad y un grupo de estaciones de trabajo sobre las que se ejecutan diversas herramientas de informática forense. La aplicación coordinara las actividades operativas y la transferencia de información digital sobre un conjunto de dispositivos de almacenamiento en red en los que se resguardan las fuentes de evidencia digital y los resultados que vayan obteniéndose del procesamiento de datos. El software para gestión automatizada de actividades operativas posibilita el procesamiento en forma simultánea y autónoma de múltiples fuentes de evidencia digital correspondientes a diferentes casos en trámite en un laboratorio de informática forense. Así mismo se permite administrar a través de una interfaz web y permite programar, controlar y notificar los avances tareas automatizadas que se ejecutan sobre el material probatorio. Los resultados de aquellos trabajos finalizados se almacenan en una base de datos y luego de ser validados quedan disponibles y accesibles a través de un sistema de consulta online para que los operadores judiciales dispongan de informes de análisis forense y otros hallazgos potencialmente relevantes que les permitan una evaluación oportuna de la evidencia digital sometida a peritaje.

CAPÍTULO 7: Conclusiones y Recomendaciones

Conclusiones

1) El Perito informático debe regir su accionar con las buenas prácticas impartidas por los estudios en la materia y que se resumen en la metodología propuesta, en lo referente al tratamiento de la prueba digital y a su procedimiento de preservación, manipulación y análisis; para de algún modo encuadrar la actividad en un marco de legalidad conforme la normativa del Ecuador.
2) Es necesaria una legislación que se adecue a esta nueva situación. También, que los actores judiciales reciban la capacitación acorde para enfrentarse con más delitos de este tipo y las situaciones que conllevan. En este sentido, resulta crucial una revisión que permita realizar las reformas pertinentes para regular las prácticas de pericias informáticas, incorporando la prueba digital y todo lo que ella implica.
3) Los crímenes cibernéticos están distribuidos entre actos de motivaciones financieras, actos relacionados con contenidos informáticos, actos contra la confidencialidad contra la confidencialidad, integridad y accesibilidad de los sistemas informáticos. Cada vez aumentan los ciber delincuentes explotando la comodidad, velocidad y anonimato que brinda el Internet para cometer sus fechorías. Consecuentemente, causan gran impacto en la sociedad produciendo daños graves que representan amenazas muy reales para las víctimas en el Ecuador y el mundo.
4) La metodología llevada por los peritos informáticos de la provincia de Pichincha hasta el momento no comprende una correcta estructura ni las validaciones necesarias para asegurarse que las evidencias digitales tomadas para el proceso de investigación no hayan sido manipuladas por terceros.
5) El informe pericial es muchas veces una prueba importante en el juzgamiento de comportamientos delictivos mediante el uso de TICs a través de ayudar a identificar al emisor, ubicar los rastros que dejó el emisor como la dirección electrónica, dirección IP del computador utilizado, funciones de un usuario en un sistema, etc. identificar domicilio de los dispositivos involucrados (servidores, computadores) y ayudar a identificar al autor principalmente.
6) La metodología planteada es una solución a la problemática que actualmente vive nuestra sociedad con herramientas que están disponibles en el mercado y procedimientos de seguridad de la información, que pueden apoyar la actividad de los Peritos y asegurar el uso de la prueba digital en el juzgamiento de los delitos.
7) Los perpetradores de delitos cibernéticos ya no requieren aptitudes o técnicas complejas. En particular, en el contexto de los países en desarrollo han surgido subculturas de jóvenes que participan en fraudes financieros informáticos.
8) La aportación de una prueba digital en cualquier juicio es cada vez más habitual: comentarios en redes sociales, videos y fotografías, grabaciones de videovigilancia,

mensajería instantánea, correos electrónicos, archivos de discos externos, registros (logs) de sistemas informáticos de equipos electrónicos, principalmente. Pero esta gran variedad de fuentes probatorias debe tener acceso al proceso judicial para convertirse en prueba. Del análisis a los informes periciales se determinó la importancia de la prueba digital, se hizo una investigación de las herramientas tecnológicas y procedimientos que se disponga sobre la investigación de delitos a través del uso de TICs.

9) Solamente la educación y la responsabilidad en el uso que se hace de la tecnología y del Internet resultan fundamentales para formar usuarios conscientes de estos peligros.
10) Puede considerarse a la evidencia digital como un tipo de prueba física en donde sus datos pueden ser recolectados, almacenados y analizados con herramientas informáticas forenses y técnicas especiales.
11) Un porcentaje considerable de denuncias pertenecen a una serie de conductas identificadas que ponen en riesgo la integridad física y emocional de los usuarios afectados como el CiberBullying.
12) En el Ecuador según el Ministerio de Telecomunicaciones existen 8,67 millones de usuarios de internet, que representan un atractivo para individuos que buscan una oportunidad para delinquir y defraudar por medio del uso de las TICs. ante el crecimiento constante de estas, y el "boom" del Internet al que acceden adultos, jóvenes adolescentes y niños con un solo clic; solamente la educación y la responsabilidad en el uso que se hace de la tecnología y del Internet resultan fundamentales para formar usuarios conscientes de estos peligros. No existen soluciones de seguridad definitivas, por lo que todas las empresas o personas, sin importar el giro, tamaño o ubicación son susceptibles de recibir ataques informáticos.
13) Las causas que más atienden los Peritos informáticos son verificación de mensajes utilizando correos electrónicos, investigación de estafas, calumnias, publicaciones en sitios web, identificación del origen de comentarios calumniosos y de deshonra en redes sociales. El 45% de las pericias se refieren a buscar la extracción y análisis de contenidos de evidencias recopiladas en medios físicos.
14) Con base en las normas ISO 27037 Y 27042 se ha propuesto una metodología para manejo de prueba digital en base a metodologías de análisis e informática forence que debería aplicarse para el desarrollo de las pericias informáticas en el Ecuador. En esta metodología se han especificado las actividades a cumplir en cada una de las fases, las que son resultado del estudio de las experiencias aplicadas por otros países.

Recomendaciones

1) Se recomienda que las personas acreditadas como Peritos informáticos en la República del Ecuador cuenten con acceso a laboratorios forenses que tengan implementadas las herramientas descritas.
2) Se recomienda usar las funciones más efectivas en las herramientas forenses. Estas son Análisis de datos, Base de datos, Recuperación de archivos eliminados, Imágenes de disco, Análisis de correo electrónico.
3) Dado que la penetración de Internet en Sur América es del 73%, se recomienda a las instituciones públicas están a la vanguardia en lo que se refiere a tecnología.
4) Se recomienda mantener discreción con las redes sociales, debido a que la mayor parte de juicios analizados las involucran. Tomando en cuenta que el número de usuarios de redes sociales en todo el mundo ha aumentado a casi 3,5 mil millones a principios de 2019.
5) Se recomienda a los Peritos informáticos tener buenas prácticas. en sus metodologías, ya que la aportación de una prueba digital en cualquier juicio es cada vez más habitual
6) El Perito Informático debe ser muy cuidadoso y cumplir con los proceso y protocolos que establece la informática forense y la normativa jurídica del Ecuador, para que no se contamine la evidencia digital y pueda ser considerada prueba en un Juicio.
7) Para poder manejar toda la información de una posible evidencia y para que esta pueda ser empleada en un proceso judicial, se recomienda tener métodos donde cada proceso esté documentado con bases de seguridad y análisis de riesgos.
8) Varios países como Estados Unidos, México, Argentina han establecido metodologías para la investigación de forense de delitos cibernéticos. El Ecuador ha formulado un Manual de Manejo de Evidencias Digitales y Entornos Informáticos de la Fiscalía General que si bien es de uso regular en la Policía Judicial y Fiscalía no se aplica en las pericias realizados por peritos particulares calificados al Consejo del a Judicatura conforme se desprende del análisis a los informes periciales elaborados por los mismos. Únicamente un 16% siguen una metodología o procedimientos de análisis forense adecuados y de estos solo el 40% cuentan con las herramientas de informática forense necesarias para una tarea profesional de investigación. Dicho esto, se recomienda estandarizar las metodologías a ser usadas en el país.
9) La ISO/IEC 27000 es un conjunto de estándares que incluyen las mejores prácticas en el área de la seguridad de la información. Dentro de esta familia de estándares, existen estándares específicos que se recomienda para profundizar prácticas de la informática forense tales como ISO/IEC 27041 (2015), ISO/IEC 27037 (2012), ISO/IEC 27017 (2015), ISO/IEC 27050 (2017), ISO/IEC 27042 (2015).

Glosario de Términos

C

Cicero
Es una herramienta que permite gestionar de forma específica el acto del Juicio Oral.....68, 78

D

delito informático
Son todos aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal. 8, 9, 28, 30, 31, 50

F

FTK
Es una herramienta de análisis forense y creación de imágenes disponible en la Web de AccessData.....17, 60, 73, 97

G

GPS
Sistema de Posicionamiento Global es un dispositivo electrónico que obtiene las posiciones en tierra mediante la triangulación de señales satelitales, luego envía esos datos a un software de rastreo mediante el módulo GSM/GPRS usando la red de operadoras celulares. 138

H

HASH
Se llaman funciones hash a algoritmos matemáticos que se utilizan en el área de la criptografía para ayudar a identificar que no se haya modificado datos en un archivo. 49

I

Imagen forense
Es el resultado de aplicar técnicas que permiten crear una copia exacta del archivo o equipo original en uno nuevo. Esto significa que el original y la copia serán idénticos al momento preciso en que se hizo la imagen. 68
Integridad
Propiedad que busca mantener los datos libres de modificaciones no autorizadas .. 7, 8, 9, 34, 38, 39, 40, 41, 43, 63, 68, 69, 73, 74, 87, 88

M

Malware
Cualquier programa o mensaje, susceptible de causar perjuicios a los usuarios de sistemas informáticos. 34
MD5
Es un algoritmo de reducción criptográfico de 128 bits ampliamente usado. Uno de sus usos es el de comprobar que algún archivo no haya sido..... 49, 69, 72, 74, 86

N

S

T

U

Bibliografía

ACFE. (2019). *ACFE*. Obtenido de https://www.acfe.com/cfe-qualifications.aspx

Acurio, S. (2009). Obtenido de https://www.oas.org/juridico/english/cyb_pan_manual.pdf

Acurio, S. (2017). *Delitos Informáticos.* Obtenido de OAS: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Aranzadi. (2012). *Delincuencia informática: tiempos de cautela y amparo.* Navarra: España: Editorial: Andalucía.

Asamblea Nacional. (10 de 02 de 2014). *COIP.* Obtenido de https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/ECU/INT_CEDAW_ARL_ECU_18950_S.pdf

Avira Operations GmbH & Co. KG., ". d. (2019).

Baquerizo, J. Z. (1998). *Delitos Informáticos en el Ecuador.* EDINO.

Barrio, M. (2018). Las direcciones IP se agotan, y ahora llega el problema de IPv6. *El Pais*. Obtenido de https://retina.elpais.com

Bendinelli, M. (2014). Delitos informáticos. La importancia de la prueba digital en el proceso judicial. *Micro Juris*. Obtenido de https://aldiaargentina.microjuris.com

Camacho, L. (1987). *Es delito informático.* Obtenido de https://s3.amazonaws.com/academia.edu.documents/38639962/cyb_ecu_delitos_inform.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1525655191&Signature=WBj2wqsdMpY43fyzUyRlPYymgKk%3D&response-content-disposition=inline%3B%20filename%3DDr._Santiago_Acurio_Del

Cobarrubias, V. (2009). *Protocolo Informático Forenses* . Obtenido de Ciencia Forense Informática: http://forenseinformatico.blogspot.com/

Conde O'Donnell, H., & González P., C. y. (2009). El delito Informatico.

Coronel, B. (2018). *recolección de evidencia forense.* Cuenca: Universiddad de Cuenca.

DATAREPORTAL. (2019). *Digital 2019 Ecuador (January 2019) v01.* Obtenido de https://datareportal.com/reports/digital-2019-ecuador

Dynek, J. (2018). *National Cybersecurity Student Association*. Obtenido de https://www.cyberstudents.org/blog-post/popular-forensic-software/

FBI. (2018). *FBI.gov*. Obtenido de https://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm

Fonrensic, E. (2019). *Enterprise Content Meets Forensic Security*. Obtenido de https://www.guidancesoftware.com/

Gutiérrez, J., & Zuccardi, G. (2006). *Informática Forense.* Obtenido de javeriana.edu.ec: http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

Herrera, H., & Leopoldo, G. (2018). Gestión automatizada de actividades operativas en laboratorios de informática forense. *SID, Simposio Argentino de Informática y Derecho 47 JAIIO*, 24-35.

International Telecommunication Union. (2018). *Measuring the Information Society Report 2018 – Volume 1.*

INTERPOL. (2018). *Ciberdelincuencia*. Obtenido de https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

ISO/IEC. (2012). *Organisacion International de Normalizacion*. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en

ISO/IEC. (2015). *Organizacion Internacional de Normalizacion*. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27042:ed-1:v1:en

IT-Security. (09 de 2013). *IT-INSECURITY*. Obtenido de http://insecurityit.blogspot.com.

Jara, L., & Ferruzola, E. (2017). Delitos a través de redes sociales en el Ecuador: Una aproximación a su estudio. *RIDTEC*.

Jésus Loredo, A. R. (2013). Delitos Informaticos: Su clasificación y una visión general de las medidas de acción para combatirlo . *Investigación-Seguridad en TI* .

Jesus, D. d., & Milagre, J. A. (2018). Manual de crimes informáticos. *Revista de Direito UNIFACEX*.

Jhony Enriquez, Y. A. (2015). Los delitos informaticos y su penalización en el Código Organico Integral Penal ecuatoriano . *SATHIR CITT - UPEC*.

Kemp, S. (2019). *We Are Social.* Global Consultant.

Krause, J. (2019). *Forensic Control*. Obtenido de https://forensiccontrol.com/resources/beginners-guide-computer-forensics/

Leonardo, S. (Agosto de 2014). Los Delitos Informáticos que afectan a los usuarios del Sistema Nacional de Contratación Pública. Ecuador: UNIVERSIDAD CENTRAL DEL ECUADOR.

Lerena, R., Podestá, A., & Constanzo, B. (2016). *Guía Integral de Empleo de la Informática Forense en el Proceso Penal .* Obtenido de InF-Lab: http://redi.ufasta.edu.ar:8080/xmlui/bitstream/handle/123456789/1592/PAIF.pdf?sequence=1

Llangari, A. (2016). *ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y DE TELECOMUNICACIONES EN EL ECUADOR bajo las nuevas normas jurídicas.* Quito: ESPE.

López, O., Amaya, H., & León, R. (2004). *INFORMÁTICA FORENSE: GENERALIDADES, ASPECTOS TÉCNICOS Y HERRAMIENTAS.* Obtenido de http://www.urru.org/papers/Rrfraude/InformaticaForense_OL_HA_RL.pdf

Maldonado, D. (2015). Los delitos informáticos y la ciberseguridad. *policia de Investigaciones de Chile.*

Martínez, A. (2014). *INCIBE-CERT.* Obtenido de INCIBE: https://www.incibe-cert.es/blog/rfc3227

Mera, D., & Benavides, V. (2018). ANÁLISIS DE BRECHAS DEL PROCESO DE COMPUTACION FORENSE DEL ECUADOR. *UESS*.

NIJ. (2004). *US Departament Justice*. Obtenido de https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

NUIX. (2019). *NUIX.COM*. Obtenido de https://view.ceros.com/nuix/nuix-total-data-intelligence/p/25

ONU. (2013). Cybercrime Study. *Estudio Exhaustivo sobre el delito cibernético.* New York: Oficina de las Naciones Unidas contra el delito.

Proaño, M. (2012). *Repositorio PUCE.* Obtenido de http://repositorio.puce.edu.ec/bitstream/handle/22000/7891/9.56.001143.pdf?sequence=4&isAllowed=y

Robles, S. (2015). *Forensic Focus*. Obtenido de Magnet IEF: https://www.forensicfocus.com/c/aid=138/reviews/2015/magnet-ief/

Rodriguez, J. (2012). Análisis de los delitos informáticos presentes en las redes sociales en Colombia. *UniLibre*. Obtenido de http://bdigital.ces.edu.co

Security, P. (2013). Obtenido de Security, S.L. "Panda Security": http://pandasecurity.com

Serna, A. F., Rivera, O. D., & Morales, J. D. (2012). FRAMEWORK PARA LA COMPUTACIÓN FORENSE EN COLOMBIA.

Snyder, J. (2018). *TechnologyINT*. Obtenido de Forensic Toolkit® (FTK®): Reconocido alrededor del Mundo como el Estandar en Software de Informática Forense.: http://technoint.weebly.com/software-de-anaacutelisis-informaacutetico-forensic-tool-kit-ftk.html

Zuccardi, G., & Gutiérrez, J. D. (2006). *Informática Forense* . Obtenido de http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf

Martínez, J. (2009). Computación forense: descubriendo los rastros informáticos. México DF, México. Editorial: Alfaomega

Casey Eoghan. (2005). Handbook of Computer Crime Investigation, Forensic Tools and Technology. Estados Unidos: Academic Press.