MAESTRÍA EN CRIMINALÍSTICA

# TRABAJO FIN DE MAESTRÍA

TÍTULO: "EL INFORME CRIMINOLÓGICO FORENSE EN LOS DELITOS INFORMÁTICOS"


Alumno: Mirian Alexandra Zambrano Bravo.

Tutor: Dra. Jacqueline Guerrero Carrera.


Quito, mayo de 2022.

# AUTORÍA DEL TRABAJO

Las ideas, contenidos y conclusiones expuestos en el presente trabajo académico, son de exclusiva responsabilidad del autor.

Quito, mayo de 2022.

Firmado electrónicamente por:
MIRIAN ALEXANDRA
ZAMBRANO BRAVO

f ……..

Mirian Alexandra Zambrano Bravo

## AUTORÍA DE DERECHOS DE PROPIEDAD INTELECTUAL

Autorizo a la Universidad Internacional del Ecuador, la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Quito, mayo de 2022.

Firmado electrónicamente por:
MIRIAN ALEXANDRA ZAMBRANO BRAVO

f .....

Mirian Alexandra Zambrano Bravo

***Agradecimiento***

*Principalmente a Dios por otorgarme sabiduría y la salud para la culminación del presente trabajo, al apoyo incondicional de mis padres e hijos, que son el motivo de inspiración y motor de vida; y a mis amigos por su especial colaboración durante el desarrollo del este trabajo.*

***Un profundo y sincero "GRACIAS".***

## ÍNDICE GENERAL

**AGRADECIMIENTO** ..... **IV**
**ÍNDICE GENERAL** ..... **V**
**ÍNDICE DE TABLAS** ..... **VI**
**ÍNDICE FIGURAS** ..... **VII**
**ÍNDICE ANEXOS** ..... **VIII**
**RESUMEN** ..... **IX**
**ABSTRACT** ..... **X**

**INTRODUCCIÓN**.....14
**CAPÍTULO I** ....16
EL PROBLEMA .....16
1.1 Planteamiento del problema .....16
1.2 Formulación del problema .....17
1.3 Objetivos .....17
1.3.1 Objetivo general .....17
1.3.2 Objetivos específicos .....17
1.3 Justificación .....18

**CAPÍTULO II** .....19
MARCO TEORICO - "DE LOS DELITOS INFORMÁTICOS Y SU INVESTIGACIÓN" .....19
2.1 Antecedentes ..... .....19
2.2 Investigación de los delitos informáticos ..... 20
2.2.1 Generalidades de los delitos informáticos ..... 20
2.2.1.1 Tipificación de los delitos informáticos .....22
2.2.1.1.1 Tipificación e infracciones informáticas en Ecuador .....24
2.3 Informática forense ..... 30

2.3.1 Evidencia digital ..... 31
2.3.2 Cadena de custodia ..... 32
2.3.3 Ciclo de la investigación forense ..... 33
2.3.3.1 Identificación de incidentes y solicitud forense ..... 35
2.3.3.2 Recopilación y adquisición de la evidencia digital ..... 37
2.3.3.2.1 Guía de mejores prácticas de computación forense ..... 38
2.3.3.2.2 Norma ISO/IEC 27037:2012 ..... 39
2.3.3.2.3 Norma ISO/IEC 27042:2015 ..... 41
2.3.3.3 Preservación de la evidencia digital ..... 43
2.3.3.4 Análisis de la evidencia digital ..... 44
2.3.3.5 Documentación y resultados ..... 46
2.3.3.5.1 Informe Técnico ..... 47
2.3.3.5.2 Informe Ejecutivo ..... 48

**CAPÍTULO III** ..... 49
"DEL INFORME TÉCNICO PERICIAL INFORMÁTICO" ..... 49
3.1 Peritaje informático..... 49
3.1.1 Importancia de la pericia ..... 51
3.1.2 Prueba valor probatorio ..... 51
3.1.2.1 Prueba electrónica ..... 52
3.2 Peritaje informático..... 53
3.2.1 Normativa relacionada con el peritaje informático ..... 54
3.2.1.1 Obligaciones de los peritos en el Ecuador ..... 55
3.2.2 Servicios de los peritos informáticos ..... 56
3.3 Informe técnico pericial ..... 57

**CAPÍTULO IV** ..... 61
CONCLUSIONES Y RECOMENDACIONES ..... 61
4.1 CONCLUSIONES ..... 61
4.2 RECOMENDACIONES ..... 62
BIBLIOGRAFÍA ..... 65

## ÍNDICE DE TABLAS

**CAPÍTULO II** ……19

**Tabla 2.1.1.1.1:** Tipificación de los delitos informáticos ……23

**Tabla 2.2.1.1.1.1:** Tipificación de los delitos informáticos en Ecuador.. ……30

**Tabla 2.3.3.2.1.1:** Guía de mejores prácticas de computación forense ……39

**CAPÍTULO III** ……49

**Tabla 3.2.1.1:** Normativa en relación a la pericia ……55

**Tabla 3.3.1:** Contenido del informe pericial ……59

## ÍNDICE DE FIGURAS

**CAPÍTULO II** …..……..19

**Figura 2.3.3.1:** Fases del análisis forense digital ……..……..35

**Figura 2.3.3.1.1:** Identificación de Incidentes y solicitud forense ……..…....36

**Figura 2.3.3.2.1:** Recopilación y adquisición de la evidencia digital ...……..….37

**Figura 2.3.3.2.2.1:** Etapas de la norma ISO 27037:2012 ……..……....40

**Figura 2.3.3.3.1:** Preservación de la evidencia digital ……..……..……....44

**Figura 2.3.3.4.1:** Análisis de la evidencia digital ……..……....44

## ÍNDICE DE ANEXOS

**CAPÍTULO II** .....19

**ANEXO A:** Guía de mejores prácticas de computación forense .....75

**CAPÍTULO III** .....49

**ANEXO B:** Modelo informe pericial .....79

**ANEXO C:** Investigación de Campo (Casuística) .....82

**RESUMEN**

Desde la aparición de las tecnologías de la información y comunicación (TIC) a nadie se le escapa la enorme influencia que ha alcanzado en la vida diaria de las personas y organizaciones, lo que ha conllevado que las personas modifiquen su manera de interactuar afectando profundamente a la sociedad. Así también, el aumento de la demanda del uso de las tecnologías y la fácil asequibilidad conlleva a que los intrusos y a la delincuencia organizada encuentren diversas formas de transgredir la ley.

Conforme se va incrementando y variando la utilización de los recursos y herramientas tecnológicas, las amenazas y vulnerabilidades son permanentes en la vida diaria de la sociedad ecuatoriana, los intrusos informáticos conocen cada vez con más profundidad los detalles de las tecnologías, seguridades y sus limitaciones, lo que les convierte en expertos manipuladores de la información, por ello, es cada vez más fácil desaparecer la evidencia y confundir a los investigadores.

Bajo este contexto, el presente trabajo de investigación tiene como objetivo, analizar el rol que cumple el informe técnico pericial informático en el procedimiento de investigación de actos ilícitos cometidos mediante la utilización de medios tecnológicos en Ecuador, así como su problemática e incidencia en el procedimiento judicial.

Consecuentemente se identificará las técnicas y metodologías empleadas para la elaboración del informe técnico pericial informático acorde a las Guías Internacionales y Norma ISO/IEC: 27037:2012 - 27042: 2015, así como las herramientas utilizadas tanto por los infractores como por los investigadores, además se pretende evidenciar las ventajas de la aplicación de las Guías Internacionales y la Norma ISO/IEC: 27037:2012 - 27042: 2015 en la gestión de la

evidencia digital, a fin de contribuir a que la investigación se desarrolle dentro de los marcos regulados, controlados y con uso de tecnología apropiada.

**PALABRAS CLAVE:**

- DELITOS
- DELITOS INFORMÁTICOS
- NORMA ISO/IEC: 27037: 2012 - 27042: 2015
- INFORME TÉCNICO PERICIAL INFORMÁTICO

**ABSTRACT**

Since the appearance of information and communication technologies (TIC) no one is unaware of the enormous influence that it has reached in the daily life of people and organizations, which has led people to modify their way of interacting, profoundly affecting the society. Likewise, the increase in demand for the use of technologies and their easy affordability means that intruders and organized crime find various ways to break the law.

As the use of technological resources and tools increases and varies, threats and vulnerabilities are permanent in the daily life of Ecuadorian society, computer intruders know more and more in depth the details of technologies, security and their limitations, which makes them expert manipulators of information, therefore, it is increasingly easy to disappear the evidence and confuse the investigators.

In this context, the present research work aims to analyze the role played by the computer expert technical report in the investigation procedure of illegal acts committed through the use of technological means in Ecuador, as well as its problems and incidence in the procedure. judicial.

Consequently, the techniques and methodologies used for the preparation of the computer expert technical report will be identified in accordance with the International Guides and ISO / IEC Standard: 27037: 2012 - 27042: 2015, as well as the tools used by both offenders and investigators, in addition it is intended to demonstrate the advantages of the application of the International Guides and the ISO/IEC Standard: 27037: 2012 - 27042: 2015 in the management of digital evidence, in order to contribute to the development of research within regulated frameworks, controlled and with the use of appropriate technology.

**KEYWORDS:**

- CRIMES
- CYBERCRIME
- ISO/IEC STANDART: 27037: 2012 – 27042: 2015
- COMPUTER EXPERT TECHNICAL REPORT

# INTRODUCCIÓN

Vivimos inmersos en un mundo tecnológico, puesto que utilizamos la tecnología en nuestro día a día, en prácticamente todas las actividades de nuestra vida. En ese contexto la información tiene un rol transcendente y actualmente uno de los bienes más importantes. Desde la aparición de las Tecnologías de la Información y Comunicación (TIC) es irrefutable la enorme influencia que ha alcanzado en la vida diaria de las personas y organizaciones que hacen uso de estos medios y sistemas informáticos para la ejecución de sus operaciones y almacenamiento de datos.

Sin embargo, también es evidente el inescrupuloso que se hace de las tecnologías de Información y comunicación (TIC), lo que afecta profundamente a la sociedad. Así también, el aumento de la demanda del uso de las tecnologías y la fácil asequibilidad conlleva a que los intrusos y a la delincuencia organizada encuentren diversas formas de transgredir la ley.

Conforme se va incrementando y variando la utilización de los recursos y herramientas tecnológicas, las amenazas y vulnerabilidades son permanentes en la vida diaria de la sociedad ecuatoriana, los intrusos informáticos conocen cada vez con más profundidad los detalles de las tecnologías, seguridades y sus limitaciones, lo que les convierte en expertos manipuladores de la información, por ello, es cada vez más fácil desaparecer la evidencia y confundir a los investigadores.

Además, un factor preponderante en la violación a las seguridades tecnológicas es la carencia en la cultura sobre seguridad informática que existe en los usuarios y consumidores de servicios tecnológicos. Dentro de ataques e incidentes más comunes tenemos: troyanos, virus y gusanos, backdoors, robo de contraseñas, correo no deseado, ataques de denegación de servicio (DOS), sniffing, buffer overflow e IP spoofing, phishing, entre otros.

Con la finalidad de encontrar y determinar las posibles causas de este tipo de ataques y/o actos maliciosos considerados como delitos informáticos, existe la Informática forense como vía clave para la investigación de estas prácticas ilícitas,

llegando a ser una disciplina complementaria para la justicia, misma que permite aplicar técnicas científicas y analíticas para identificar, analizar, preservar la evidencia digital.

La investigación de la delincuencia informática, no es tarea fácil, ya que la mayoría de los datos probatorios son intangibles, los cuales pueden ser volátiles y de vida corta. En este sentido el tratamiento, mantenimiento y preservación de la evidencia digital juega un papel fundamental en cuanto a evitar la manipulación y falsificación durante el proceso judicial con el fin de acreditar su autenticidad.

En el capítulo uno se detalla los elementos principales del tema de investigación, tales como: planteamiento del problema, formulación de problema, objetivo general y específicos, así como la justificación de este trabajo.

En el capítulo dos se abordan los temas relacionados con el marco teórico de los delitos informáticos, informática forense, aplicación de procedimientos y métodos en el análisis forense digital, guía de mejores prácticas de computación forense, así como la aplicación de la Norma Internacional ISO/IEC: 27037:2012 - 27042: 2015.

En el capítulo tres se aborda el peritaje informático e importancia; la prueba electrónica; el perito forense informático, sus obligaciones y servicios; y, la normativa relacionada con el peritaje.

En el capítulo cuatro constan las conclusiones y recomendaciones en cuanto al trabajo de investigación realizado.

.

# CAPÍTULO I
# EL PROBLEMA

## 1.1 Planteamiento del problema

El progreso tecnológico que día a día va experimentando el mundo y la sociedad ecuatoriana, supone a la vez una evolución en las distintas formas de infringir la ley, en relación con las diversificaciones de los delitos y la aparición de actos ilícitos.

Actualmente no existe una seguridad total para los usuarios y consumidores de los servicios tecnológicos debido a la complejidad del entorno virtual, lo que conlleva a que exista mayor incidencia de denuncias por delitos informáticos. Por esta razón la Fiscalía y la Policía realizan innumerables esfuerzos para capacitar a su personal sobre cómo detectar esta forma de delinquir, formando profesionales con altos conocimientos respecto de la aplicación de procedimientos científicamente probados, válidos y reconocidos a nivel nacional e internacional, sobre las evidencias que vulneran los sistemas informáticos.

Es preciso considerar que la falta de infraestructura, procedimientos, conocimientos, herramientas modernas e implementos tecnológicos adecuados y claros, en cuanto a la aplicación de las Guías Internacionales y de la Norma ISO/IEC: 27037:2012 - 27042: 2015, para la gestión de la evidencia digital en los entes u organismos de control, traen como consecuencia que la investigación informática no se realice de forma óptima, ya que la mayoría de los datos probatorios son intangibles, los cuales pueden ser volátiles y de vida corta, por tal razón el investigador juega un papel fundamental en ejecutar la correcta recolección de la información, tanto visible como oculta, relacionada con el hecho de la investigación.

El investigador deberá aplicar procedimientos, como técnicas y herramientas disponibles para obtener, custodiar, revisar, analizar, preservar y presentar la evidencia digital encontrada en una escena del delito, lo que permitirá garantizar la

autenticidad y seguridad de la información a fin de fortalecer el valor probatorio ante los organismos competentes para la resolución de los delitos.

## 1.2 Formulación del problema

El investigador, dentro de la gestión de la evidencia digital, debe realizar el procedimiento de documentación y presentación de los resultados obtenidos en el trayecto de la investigación, para lo cual elabora el informe técnico pericial informático. Este contiene una declaración pormenorizada del análisis realizado y detalla los siguientes aspectos: metodología, técnicas y el compendio de los hallazgos encontrados. Por consiguiente, el investigador es el responsable de emitir conclusiones objetivas e imparciales, contenidas en el informe que debe ser incorporado como prueba en los procesos judiciales.

La falta de infraestructura, procedimientos, conocimientos, herramientas modernas e implementos tecnológicos adecuados y claros, así como a la aplicación de las Guías internacionales y de la Norma ISO/IEC: 27037:2012 - 27042: 2015, para la gestión de la evidencia digital en los entes u organismos de control, constituye una debilidad al momento de elaborar el informe técnico pericial informático, lo cual puede llegar a afectar la validez de la evidencia digital, que debe ser presentada ante un tribunal de justicia.

## 1.3 Objetivos

### 1.3.1 Objetivo general

- Analizar el rol que cumple el informe técnico pericial informático en el procedimiento de investigación de actos ilícitos cometidos mediante la utilización de medios tecnológicos en Ecuador, así como su problemática e incidencia en el procedimiento judicial.

### 1.3.2 Objetivos específicos

- Identificar las técnicas y metodologías empleadas para la elaboración del informe técnico pericial informático acorde a las Guías Internacionales y

Norma ISO/IEC: 27037:2012 - 27042: 2015, así como las herramientas utilizadas tanto por los infractores como por los investigadores.

- Evidenciar las ventajas de la aplicación de las Guías Internacionales y la Norma ISO/IEC: 27037:2012 - 27042: 2015 en la gestión de la evidencia digital, a fin de contribuir a que la investigación se desarrolle dentro de los marcos regulados, controlados y con uso de tecnología apropiada.

### 1.4 Justificación

Con el pasar del tiempo los delitos informáticos van causado grandes pérdidas económicas y afectando la información calificada de las instituciones tanto públicas y privadas, a lo que se suma la pérdida de credibilidad y debilitamiento institucional que sufren las entidades afectadas, especialmente en el sector comercial y bancario. Al ser evidente la fragilidad tecnológica en las entidades refleja la importancia de nuestra investigación al querer demostrar los problemas en el Ecuador en cuanto al uso de las TIC y la aplicación de las Guías Internacionales, así como la Norma ISO/IEC: 27037:2012 - 27042: 2015 en cuanto al manejo de la gestión de la evidencia digital y como los organismos de control hacen frente a los delitos informáticos.

# CAPÍTULO II

# MARCO TEORICO

# “DE LOS DELITOS INFORMÁTICOS Y SU INVESTIGACIÓN”

## 2.1 Antecedentes

Desde la aparición de las Tecnologías de la Información y Comunicación (TIC) 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 Losa, 1987).

Acurio (2016) expresa que determinados enfoques doctrinales 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. A este respecto Casanoba (1987), señala que se ha ido imponiendo la expresión de delito informático, que tiene la ventaja de su plasticidad, al relacionarlo directamente con la tecnología sobre o a través de la que actúa. Sin embargo en puridad no puede hablarse de un delito informático, sino de una pluralidad de ellos, en los que encontramos como única nota común su vinculación de alguna manera con los computadores, pero ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del – hecho delictivo o merecedor de serlo – presenta siempre características semejantes … el computador es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes (el aparato, el programa, los datos almacenados).

Por lo que se ha preferido delimitar el contenido de este fenómeno, como delincuencia Informática o criminalidad informática que 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 y poner en peligro un buen jurídico cualquiera.

A estas conductas o actos ilícitos que son perpetrados mediante el uso desmedido de equipos tecnológicos, se las puede encontrar bajo las siguientes expresiones: delitos informáticos, delitos virtuales, delitos electrónicos, cybercrimenes, delitos digitales, Inforcrímenes, delitos relacionados con la computadora, delitos telemáticos, crímenes por computadora, crímenes cibernéticos, crímenes tecnológicos, delincuencia relacionada con el ordenador. Los delitos informáticos son los nuevos verdugos de esta sociedad tecnificada, al mismo tiempo que la tecnología evoluciona el delito crece.

## 2.2 Investigación de los delitos informáticos.

Para el análisis de los delitos informáticos es preciso entender cómo la criminalidad informática y los incidentes de seguridad van evolucionando en el mundo y la sociedad ecuatoriana.

Los componentes de prueba de los procesos judiciales son de absoluta relevancia, en razón que mediante el correcto desarrollo de la investigación se puede dilucidar la comprobación de la veracidad del hecho ocurrido, así como garantizar la autenticidad de la prueba. Dentro del proceso investigativo se debe mantener la formalidad y claridad de los procedimientos y/o técnicas empleadas, ya que sirven para presentar con mayor claridad y precisión las evidencias encontradas, ante el cometimiento de un delito informático.

### 2.2.1 Generalidades de los delitos informáticos.

Julio Téllez conceptualiza al delito informático en forma típica y atípica, entendiendo que en la forma típica son “las conductas típicas antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin” y la forma atípica “actitudes ilícitas en que se tienen a las computadoras, como instrumento o fin” (Téllez Valdés, 1996).

Acerca del concepto de delito informático, la doctrina no es uniforme en una categoría propia e independiente de esta clase de delitos, de esta manera en términos generales se define como: toda acción dolosa que provoca un perjuicio a personas o entidades, en cuya omisión intervienen dispositivos habitualmente utilizados en las actividades informáticas (Mata y Martín, 2001); o como aquellos actos antijurídicos, según la ley penal vigente, realizados con el empleo de un equipo automático de procesamiento de datos (Tiedemann, 1985). Dichos conceptos son bastante amplios, por lo que es preferible restringir los conceptos, como aquellos que el ordenador representa en medio de ejecución (Mata y Martín, 2001).

Se puede apreciar que la característica principal en estos delitos es la presencia del ordenador o computador como instrumento de comisión, pero, es necesario realizar una distinción pues en algunos casos el ordenador y sus aplicaciones constituyen el objeto material del delito (sobre el que recae físicamente la acción) y en otras será un mero instrumento para cometer hechos generalmente tipificados en el Código Penal (Mata). En esta línea Naciones Unidas ha señalado que la conducta en la desplegada en la comisión del delito implica la utilización de tecnologías digitales (…) se dirige a las propias tecnologías de la computación y las comunicaciones; o, incluye la utilización incidental de computadoras en la comisión de otros delitos (Naciones Unidas, 2005).

Es preciso indicar que en la actualidad no se cuenta con una conceptualización universal de delito informático, se debe enfatizar que han sido los empeños de varios especialistas que han tratado del tema y han formalizado definiciones prácticas, atendiendo contextos nacionales e internacionales. Siendo así, los Estados miembros del Consejo de Europa y los demás Estados, convencidos de la necesidad de aplicar con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la delincuencia informática, entre otras formas y encaminados a una adopción legislativa adecuada, fomentando la cooperación internacional, elabora el (Convenio de Ciberdelincuencia del Consejo de Europa, 2007), que se encuentra enfocado a los riesgo que las redes informáticas, la información electrónica que es utilizada

para cometer delitos, y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes; con la finalidad de prevenir los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, mediante la tipificación de estos actos.

Los delitos informáticos implican acciones de tipo criminal razón por la cual, se los ha ubicado en figuras típicas, tales como: falsificaciones, fraudes, hurto, suplantación, estafa, robos, entre otros, siendo imprescindible destacar que el mal uso de sistemas informáticos, redes y datos informáticos es lo que ha obligado a las Instituciones Jurídicas a fijar regulaciones en un marco legal.

#### 2.2.1.1 Tipificación de los delitos informáticos.

A fin de establecer un marco de referencia en el campo de las tecnologías y los delitos para la Unión Europea, en noviembre de 2001 se firmó en Budapest el “Convenio de Ciberdelincuencia del Consejo de Europa”, en dicho convenio una clasificación de delitos informáticos, divididos en cuatro grupos que se detalla a continuación:

| Delitos informáticos | |
|---|---|
| **1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos** | ✓ Acceso ilícito a la totalidad o a una parte de un sistema informático.<br>✓ Interceptación ilícita por medios técnicos, de datos informáticos, desde un sistema informático o dentro del mismo.<br>✓ Interferencia en los datos<br>• Actos que dañen, borren, deterioren, alteren o supriman datos informáticos.<br>• Provoquen daños graves<br>✓ Interferencia en el sistema |

| Delitos informáticos | |
|---|---|
| | • Obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.<br>✓ Abuso de los dispositivos |
| **2. Delitos informáticos** | ✓ Fraude informático<br>• cualquier introducción, alteración, borrado o supresión de datos informáticos<br>• cualquier interferencia en el funcionamiento de un sistema informático.<br>✓ Falsificación informática<br>• Introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos. |
| **3. Delitos relacionados con el contenido** | ✓ Delitos relacionados a pornografía infantil<br>• Producción, oferta, difusión, transmisión, posesión de pornografía infantil y visitas por medio de un sistema informático y/o en un medio de almacenamiento de datos informático. |
| **4. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines** | ✓ Copia y distribución de programas informáticos o piratería informática. |

**Tabla 2.1.1.1.1:** Tipificación de los delitos

**Fuente:** (Convenio de Ciberdelincuencia del Consejo de Europa, 2007).

En enero de 2008, se promulgó el "Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa", que tiene como objetivo principal criminalizar los actos de racismo y xenofobia cometidos mediante sistemas informáticos, que incluye las medidas que se debe tomar en los siguientes casos (Bernal J.S, 2003):

- Difusión de material xenófono o racista.
- Insultos o amenazas con motivación racista o xenófoba.
- Negociación, minimización burda, aprobación o injustificación del genocidio o crímenes contra la humanidad.

#### 2.2.1.1.1 Tipificación e Infracciones informáticas en Ecuador.

Las infracciones informáticas fueron tipificadas por primera vez en el Ecuador mediante reformas al Código Penal efectuadas a través del Título V, desde el artículo 57 al artículo 64, de la Ley de Comercio Electrónico, Firmas y Mensaje de Datos. En dicha ocasión se tipificaron los delitos contra la información protegida, la destrucción maliciosa de documentos, los daños informáticos, la apropiación ilícita, la estafa y la violación del derecho a la intimidad.

El Código Orgánico Integral Penal – COIP (Asamblea Nacional, 2014), publicado en el Suplemento del Registro Oficial No. 180 de 10 de febrero del 2014 y que entró en vigencia 180 días después, es decir el 10 de agosto del 2014, en su Disposición Derogatoria Novena derogó el Título V, desde el artículo 57 al artículo 64, de la Ley de Comercio Electrónico, Firmas y Mensaje de Datos, referidos anteriormente. En su lugar el COIP (Asamblea Nacional, 2014), incorpora otras figuras delictivas relacionadas con los sistemas informáticos y amplía el alcance de las infracciones informáticas contempladas en el anterior Código Penal.

A continuación, se establece una revisión de los artículos del COIP relacionados con la tipificación y penalización de los delitos informáticos:

| ***Diversas formas de explotación*** | |
|---|---|
| **Art. 103.** Pornografía con utilización de niñas, niños o adolescentes.<br>Pena Privativa de la libertad<br>(13 a 17 años) | • Fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual |

| | |
|---|---|
| Si la víctima, además, sufre algún tipo de discapacidad o enfermedad grave o incurable<br>Pena Privativa de la libertad<br>(17 a 19 años)<br><br>grado de consanguinidad o segundo de afinidad, tutor, representante legal, curador o pertenezca al entorno íntimo de la familia; ministro de culto, profesor, maestro, o persona que por su profesión o actividad haya abusado de la víctima.<br>Pena Privativa de la libertad<br>(22 a 26 años) | |
| **Art. 104.** Comercialización de pornografía con utilización de niñas, niños o adolescentes<br>Pena Privativa de la libertad<br>(10 a 13 años) | • Publique, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda por cualquier medio, para uso personal o para intercambio pornografía de niños, niñas y adolescentes. |
| ***Delitos contra la integración sexual y reproductiva*** | |
| **Art. 174.** Oferta de servicios sexuales con menores de 18 años por medios electrónicos<br>Pena Privativa de la libertad<br>(7 a 10 años) | • Utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juego en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de 18 años de edad. |
| ***Delitos contra el derecho a la intimidad personal y familiar*** | |
| **Art. 178.** Violación a la intimidad<br>Pena Privativa de la libertad | • Acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información |

| | |
|---|---|
| (1 a 3 años) | contenida en soportes informáticos, comunicaciones privadas o reservadas.<br>• Divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley. |
| ***Delitos contra el derecho a la propiedad*** | |
| ***Art. 186.*** *Estafa*<br>*Pena Privativa de la libertad*<br>*(5 a 7 años)* | • Mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera.<br><br>La pena máxima se aplicará a la persona que:<br><br>• Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.<br>• Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de las tarjetas de crédito, débito, pago o similares.<br>• Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica<br>• Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento.<br>• Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor. |
| **Art. 190**. Apropiación fraudulenta por medios electrónicos.<br>Pena Privativa de la libertad<br>(1 a 3 años) | • 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<br>• Inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes. |

| | |
|---|---|
| **Art. 191**. Reprogramación o modificación de información de equipos terminales. Pena Privativa de la libertad (1 a 3 años) | • Reprograme o modifique la información de identificación de los equipos terminales móviles. |
| **Art. 192**. Intercambio, comercialización o compra de información de equipos de terminales móviles. Pena Privativa de la libertad (1 a 3 años) | • Comercialice o compre base de datos que contengan información de identificación de equipos terminales móviles |
| **Art. 193**. Reemplazo de identificación de terminales móviles. Pena Privativa de la libertad (1 a 3 años) | • Reemplace las etiquetas de fabricación de los terminales móviles que contienen información de identificación de dichos equipos y coloque en su lugar otras etiquetas con información de identificación falsa o diferente a la originalidad. |
| **Art. 194**. Comercialización ilícita de terminales móviles. Pena Privativa de la libertad (1 a 3 años) | • Comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de telecomunicaciones. |
| **Art. 195**. Infraestructura ilícita. Pena Privativa de la libertad (1 a 3 años) | • Que posea infraestructura, programas, equipos, base de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil. |
| ***Delitos contra el derecho de la identidad*** | |
| **Art. 212.** Suplantación de identidad. Pena Privativa de la libertad (1 a 3 años) | • Cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona. |
| ***Delitos contra la seguridad de los activos de los sistemas de información y comunicación*** | |
| **Art. 229**. Revelación ilegal de base de datos. Pena Privativa de la libertad | • 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 |

| | |
|---|---|
| (1 a 3 años)<br><br>Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas<br>Pena Privativa de la libertad<br>(3 a 5 años) | voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas. |
| **Art. 230**.<br>Interceptación ilegal de datos.<br>Pena Privativa de la libertad<br>(3 a 5 años) | • Intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.<br>• Que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.<br>• Copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.<br>• Fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior. |
| **Art. 231**. Transferencia electrónica de activo patrimonial.<br>Pena Privativa de la libertad<br>(3 a 5 años) | • 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.<br>• Facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial |

| | |
|---|---|
| | a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.<br>• Falsificaciones informáticas. |
| **Art. 232**. Ataque a la integridad de sistemas informáticos.<br>Pena Privativa de la libertad<br>(3 a 5 años)<br><br>Si la infracción se comete sobre bienes informáticos destinados a la presentación de un servicio público o vinculado con la seguridad ciudadana.<br>Pena Privativa de la libertad<br>(5 a 7 años) | • Destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen.<br>• Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.<br>• Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. |
| **Art. 233**. Delito contra la información pública reservada legalmente.<br>Pena Privativa de la libertad<br>(5 a 7 años).<br><br>Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información.<br>Pena Privativa de la libertad<br>(7 a 10 años).<br><br>y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra | • Destruya o inutilice información clasificada de conformidad con la Ley.<br>• Que utilizando cualquier medio electrónico o informático, obtenga este tipo de información |

| | |
|---|---|
| infracción de mayor gravedad. | |
| **Art. 234**. Acceso no consentido aun sistema informático, telemático o de telecomunicaciones. Pena Privativa de la libertad (3 a 5 años) | • Sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar legítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos. |

**Tabla 2.2.1.1.1.1:** Tipificación de los delitos informáticos en Ecuador

**Fuente:** Código Orgánico Integral Penal (Asamblea Nacional Constituyente, 2014).

## 2.3. Informática forense.

La informática forense consiste, consiste en el empleo de métodos científicamente derivados y comprobados para preservar, recolectar, validar, identificar, analizar, interpretar, documentar y presentar evidenciar digitales con el propósito de hacer posible la reconstrucción de hechos considerados delictivos o ayudar a la prevención de actos no autorizados y capaces de provocar una alteración en operaciones planificadas de organismos y empresas (Carrier B, 2002).

Domínguez (2014) señala la parte vital en el combate contra el crimen es una investigación de medios digitales basada en métodos profesionales y buenas prácticas, a fin de que los elementos de videncia obtenidos mediante la misma puedan ser puestos a disposición de los tribunales. De ahí que sea necesario tomar en cuenta a la Informática Forense como disciplina que se encarga de la adquisición, el análisis y la valoración de elementos de evidencia digital hallados en ordenadores, soportes de datos e infraestructuras de red, y que pudieran aportar luz en el esclarecimiento de actividades ilegales perpetradas en relación con instalaciones de proceso de datos.

En relación anteriormente expuesto, la Fiscalía General del Estado es el ente rector para emitir los diferentes manuales, protocolos, instructivos y formatos del sistema especializado integral de investigación, medicina legal y ciencias forenses.

Por esa razón elaboró, el Reglamento del Sistema Especializado Integral de Investigación, de Medicina Legal y Ciencias Forenses (RSEIIMLCF), publicado en el Registro Oficial mediante Resolución FGE-2014-030 y (Manuales, Protocolos, instructivos y formatos del Sistema Especializado Integral de Investigación, de Medicina Legal y Ciencias Forenses, 2014), publicado en el Registro Oficial mediante Resolución No. 073-FGE-2014, estableciendo los protocolos a seguir para la investigación de los delitos que son fundamentales para el trabajo en la parte de informática forense (Fiscalía General del Estado, 2014).

### 2.3.1 Evidencia digital.

Se entiende como evidencia digital toda información con valor probatoria que se encuentra almacenada o transmitida de forma digital o binaria, y se aporte en un juicio. También, la evidencia digital es una serie metódica de técnicas y procedimientos para recopilar evidencia, desde equipos informáticos y diversos dispositivos de almacenamiento y medios digitales, que pueden presentarse en un tribunal de justicia en un formato coherente y significativo (Reyes, 2007).

El NIST (National Institute of Standards and Technology), la define como la aplicación de la ciencia a la identificación, recopilación, examen y análisis de datos, al tiempo que se preserva la integridad de la información y se mantiene estricta cadena de custodia (Grance, 2006).

En el Código Orgánico Integral Penal, señala en el **Art. 500.-** que el contenido digital es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico aislado, interconectado o relacionado entre sí (COIP, 2014).

La evidencia digital en los procesos judiciales adquiere gran relevancia ya que reside en la obligatoriedad de esclarecer y/o probar sucesos de naturaleza delictiva, a fin que los dictámenes periciales durante el juicio sean

eficientes y sólidos; facilitando que los jueces obtengan el conocimiento necesario a través de la información suministrada.

### 2.3.2 Cadena de custodia.

La cadena de custodia, se define como el conjunto de actividades y procedimientos secuenciales que se aplican en la protección y aseguramiento de los indicios y/o evidencias físicas y digitales, desde la localización en la escena del delito o lugar de los hechos, hasta su presentación ante el Juzgador y/o disposición final (Fiscalia General del Ecuador, 2014).

Siendo que el desarrollo de la investigación es técnico científico, la autenticidad e integridad del indicio es pieza clave, desde la recolección en la escena del delito hasta la presentación de la evidencia en el juicio, el investigador debe aplicar procesos enmarcados en instrumentos internacionales suscritos por la República del Ecuador y el Código Orgánico Integral Penal (COIP) a fin de garantizar su valor probatorio.

En tal virtud, el objetivo principal de la cadena de custodia es garantizar la preservación del lugar de los hechos, así como los indicios y/o evidencias ligadas al proceso, bajo criterios de protección, observación, fijación, recolección, embalaje, rotulación, sellado y traslado seguro a los Centros de Acopio del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses, de tal manera que los elementos considerados como evidencia no puedan ser manipulados, alterados, sustituidos, perdidos, contaminados o destruidos. Esto con la finalidad de mantener la integridad de la evidencia y constituirse en un verdadero aporte al sistema judicial.

Cabe indicar que la falta de protocolos claros sobre el manejo de la cadena de custodia, puede conllevarnos a la ineficiencia de la norma, pues al no tener las garantías claras sobre las pruebas que se puedan presentar en un proceso legal, la impunidad será el día a día de la justicia. Por tal razón será necesario capacitar constantemente a todos aquellos funcionarios sobre los cuales recae la responsabilidad de garantizar el debido proceso en todas las fases.

(COIP, 2014), señala **Art. 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 persona que interviene en la recolección, envió, manejo, análisis y conservación de estos elementos y se incluirán los cambios hecho en ellos".

El adecuado manejo de la cadena de custodia beneficia en diferentes instancias a los vinculados de manera directa e indirecta a una investigación, pues al contar con una herramienta como el informe técnico que resultará de la investigación, contribuye a generar seguridad sobre la validez de la evidencia, en el sentido de haber identificado y subsanando oportunamente posibles vulnerabilidades en el proceso de la cadena de custodia de las evidencias.

### 2.3.3 Ciclo de la investigación forense

El análisis forense digital, involucra las siguientes fases: a) Identificación; b); preservación c) obtención; d) análisis de la información y e) documentación.

Cabe indicar que existen metodologías y procedimientos bien definidos que pueden ser fácilmente adaptados al análisis forense en dispositivos móviles.

Estas metodologías consisten generalmente en la ejecución de las siguientes actividades:

- Preparar una copia de la evidencia digital
- Examinar la copia de la evidencia digital
- Analizar la información recuperada; y
- Crear un reporte describiendo los datos obtenidos.

Las herramientas, de análisis forense dentro de sus funcionalidades intenta facilitar el trabajo de investigación en cada una de sus fases, enfocados con mayor énfasis a la generación del reporte final veraz y de calidad, que permita revelar detalles de las actividades desarrolladas en el dispositivo móvil en cuestión, contestando las preguntas que normalmente son realizadas en el

análisis forense clásico que implican el: ¿qué se hizo?, ¿cómo se hizo?, ¿cuándo se hizo? (Cano, 2015) (Larry&Lars, 2012).

El investigador antes de desarrollar el análisis forense, debe realizar el siguiente cuestionamiento; la evidencia encontrada es un dispositivo móvil o dispositivo computacional, en cuanto existen diferencias entre el análisis forense de dispositivos móviles y el análisis de computadoras, debido a los siguientes factores:

- El diseño orientado a la facilidad de transporte.
- Almacenamiento en una memoria volátil contra memorias no volátiles.
- Facilidad de acceso para modificar o eliminar remotamente la información.
- Comportamiento de hibernación, suspensión de procesos cuando se apaga y vuelve a encender el dispositivo.
- Diversos tipos de seguridad que poseen los dispositivos móviles.
- La diversidad de sistemas operativos embebidos (Hoog, 2011)
- Ciclos cortos de producción para introducir nuevos dispositivos móviles con mayores prestaciones y nuevas funcionalidades.
- Riesgos de seguridad por la cantidad de aplicaciones existentes.

Factores que muestran la necesidad de investigar nuevas propuestas en el campo de la informática forense relacionada con dispositivos (Ariza Marta Romero, 2014).

Dentro de las metodologías existentes para el análisis forense podemos citas:

- Metodología del Departamento de Justicia (DOJ) de los Estados Unidos.

  El modelo DOJ no hace referencia entre los métodos forenses aplicados a computadores o algún otro dispositivo electrónico. Intenta construir un modelo general para aplicarlo a la mayoría de dispositivos electrónicos (J.H.P. Eloff, 2008).

- Metodología del Instituto SANS

  SANS (2002) es una organización cooperativa de investigación y educación para profesionales de la seguridad. El manejo adecuado de una investigación forense es clave para luchar contra los delitos informáticos, requiriendo un profundo conocimiento de muchas áreas para una investigación adecuada.

- Digital Forensics Research Workshop (DFRW)

  DFRW (2001) es un grupo dirigido por la academia más que por el modelo legal, ayuda a definir y enfocar la dirección de la comunidad científica en relación al análisis forense digital.

- Kevin Mandia y Chis Prosise

  Prosise (2003) define el proceso de análisis forense como una metodología de respuesta a incidentes.

Por consiguiente, se puede observar qué dentro del análisis forense, no existe una metodología universal que nos permita llevar a cabo una investigación, a partir de ellas se estudiará el siguiente modelo de análisis forense digital.

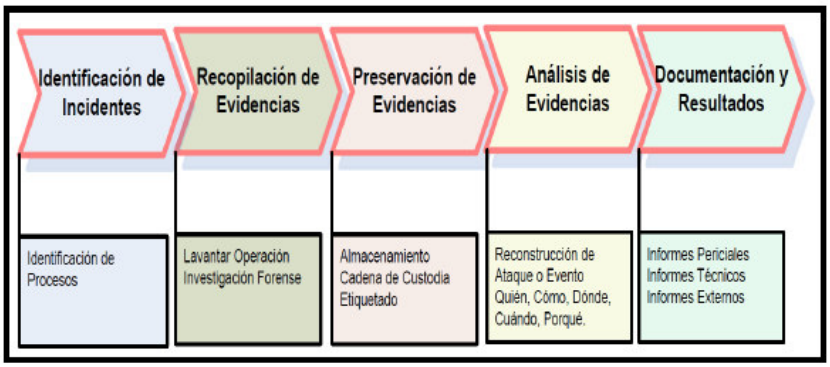


**Figura 2.3.3.1:** Fases del análisis forense digital
**Fuente:** (López, Análisis Forense Digital, 2007)

La correcta gestión de la evidencia digital, es fundamental para que sea admisible en los procesos judiciales, ya que pone en manifiesto la exigente labor que se requiere por parte de los investigadores en la informática forense, mismos

que deben aplicar procedimientos, técnicas y herramientas para obtener, custodiar, revisar, analizar y presentar la evidencia encontrada ante el tribunal, trasparentando una correcta cadena de custodia, cuyos pasos deberá desprenderse de un manual de buenas prácticas, teniendo especial cuidado en el manejo de la evidencia digital en cuanto al registro, admisibilidad, valor probatorio, preservación, transformación y recuperación, documentando las acciones realizadas y justificar todas las decisiones aplicadas en las etapas del proceso.

### 2.3.3.1 Identificación de incidentes y solicitud forense.

El investigador Inicialmente, debe confirmar la integridad de la evidencia encontrada, en esta etapa no se debe efectuar modificaciones, cambios o transformaciones, salvaguardando los requerimientos jurídicos.

Es imprescindible que el investigador se cuestione acerca de la información recogida, es decir detectar desviaciones del incidente y compararlos con acontecimientos similares en caso de existir.

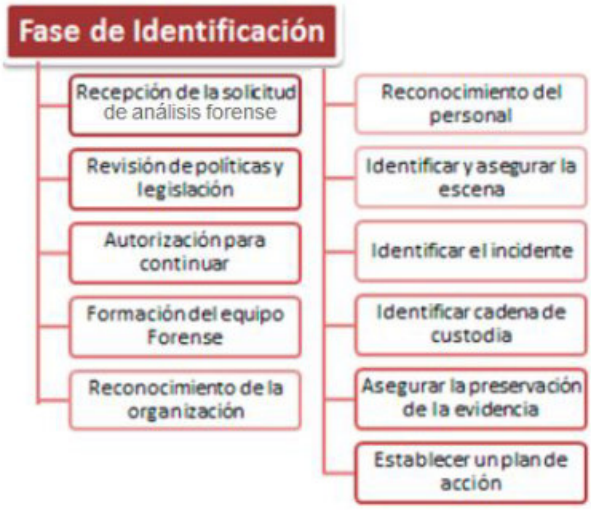


**Figura 2.3.3.1.1:** Identificación de Incidentes y solicitud forense.
**Fuente:** (Pinto, 2014).

### 2.3.3.2 Recopilación y adquisición de la evidencia digital.

En base a las pruebas realizadas en la fase inicial (Identificación de Incidentes y solicitud forense), se deberá distinguir la prioridad entre levantar la operación del sistema o efectuar una investigación forense al detalle.

Es importante considerar que se debe acondicionar el entorno de trabajo de acuerdo al estudio que se desee realizar, debiendo en la mayoría de los casos se recomienda no manipular los dispositivos originales implicados, y trabajar con imágenes, o mejor aún con una copia de éstas; hay que tener en cuenta que se necesitará montar estas imágenes tal cual estaban en el sistema comprometido (Pinto, 2014).

Consecuentemente, se inicia la investigación con la adquisición de los datos propiamente dicha, se recomienda revisar la legislación para el manejo y almacenamiento de evidencias.

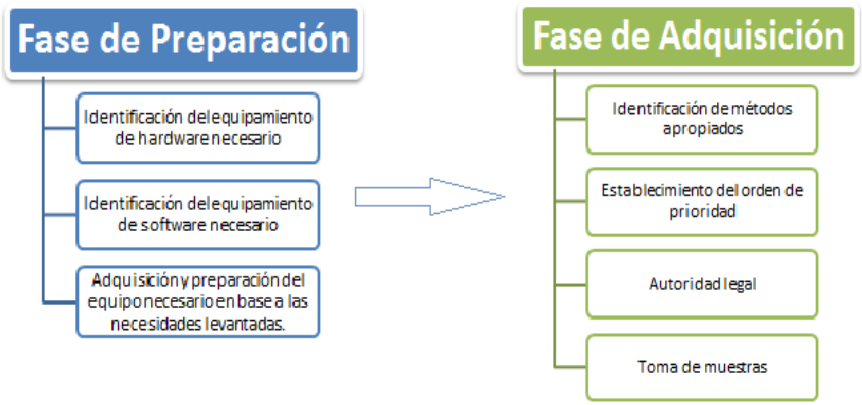


**Figura 2.3.3.2.1:** Recopilación y adquisición de la evidencia digital.
**Fuente:** (Pinto, 2014).

Es aconsejable qué en el desarrollo de la presente fase, se lleve el respectivo registro, de todas las acciones realizadas, así como los datos y/o información encontrada, debiendo procurar la mayor obtención de número de datos o información, empleándose una metodología de recopilación de evidencias.

Forma parte de la legislación ecuatoriana la Resolución No. 073-FGE-2014, por lo que estableció los Manuales, Protocolos, Instructivos y Formatos del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses, Registro Oficial Suplemento No. 318, 25 de agosto 2014, que se apega a los estándares internacionales que guía en el proceso de recolección de evidencias que guía en el proceso de recolección de evidencias (Fiscalia General del Ecuador, 2014).

#### 2.3.3.2.1 Guía de mejores prácticas de computación forense.

Las Guías para el análisis y la interpretación de la evidencia digital, garantiza o aborda cuestiones de continuidad, validez, reproductibilidad y repetividad. Además de buenas prácticas para la selección, diseño e implementación de un proceso analítico y recoger información necesaria que permita que los procesos puedan ser sometidos a escrutinios independientes cuando es caso lo requiera.

No todas las guías, se deben entender de forma estricta en cada uno de los pasos de la investigación forense, pero siempre que los elementos sean aportado y analizados como prueba dentro de un proceso judicial deben cumplir con todos los pasos previstos, tanto en la cadena de custodia como en el ciclo de la investigación forense.

A continuación, se pone a consideración las guías más reconocidas a nivel mundial en relación a las mejores prácticas en computación forense. (ANEXO - A).

| Guía | Patrocinador | Distribución |
|---|---|---|
| RFC 3227 - Recolectar y archivar evidencia | Network Working Group http:// www.ietf.org | Libre |
| Guía IOCE – Mejores prácticas en el examen forense tecnología digital | International Organization on Computer Evidenc http:// www.iece.org | Libre |

| Guía | Patrocinador | Distribución |
|---|---|---|
| Guía DoJ 1 - Investigación en la escena del crimen electrónico | U.S. DoJ http:// www.usdoj.gov | Libre |
| Guía DoJ 2 - Examen forense digital | U.S. Departament of Justice http:// www.usdoj.gov | Libre |
| Guía Hong Kong - Computación Forense - Parte 2: Mejores Prácticas | SWGDE – Scientific Working Group on Digital Evidence http:// www.acpo.police.uk | Libre |
| Guía Reino Unido - Buenas prácticas para evidencia basada en Computadores | ACPO – Association of Chief Police Officers http:// www.acpo.police.uk | Libre |
| Guía Australiana-Manejo de Evidencia En IT | Estándar Australiano http:// www.unpan1.un.org | Pago |
| Norma ISO/IEC 27037:2012 | ISO/IEC http://www.iso.org | Pago |

**Tabla 2.3.3.2.1.1:** Guía de mejores prácticas de computación forense.
**Fuente:** (Watson, 2013).

### 2.3.3.2.2 Norma - ISO/IEC 27037: 2012.

Proporciona pautas para el manejo de las evidencias digitales; sistematizando la identificación, recolección, adquisición y preservación de las mismas. Estos procesos deben diseñarse para mantener la integridad de las evidencias y con una metodología aceptable para contribuir con su admisibilidad en los procesos legales (GlobátiKa Peritos Informáticos, 2014).

La evidencia digital es gobernada por tres principios fundamentales: relevancia, la confiabilidad y suficiencia - proporciona guías para actividades específicas en el manejo de identificación, recolección, adquisición y preservación de la evidencia. Así como también, proporciona las directrices generales para la obtención de pruebas no digitales, que son necesarias en la etapa de análisis de la evidencia digital.

**Figura 2.3.3.2.2.1:** Etapas de la norma ISO 27037:2012
**Fuente:** ISO/IEC.

El objetivo primordial de la norma es, orientar a los investigadores a gestionar las evidencias digitales, con prácticas aceptadas en todo el mundo de manera sistemática e imparcial, preservando su integridad y autenticidad.

La aplicación de esta norma internacional exige el cumplimiento de las leyes, normas y reglamentos nacionales. La norma ISO/IEC 27037:2012 no hace referencia a requisitos específicos de cada jurisdicción que se refiere a cuestiones como la admisibilidad, la ponderación probatoria, la pertenencia y otras limitaciones que controlan el uso de la evidencia digital en los tribunales de justicia (GlobátiKa Peritos Informáticos, 2014).

Los principios en los que se basa la norma son los siguientes:

- Aplicación de métodos
  La evidencia digital debe ser adquirida del modo menos intrusivo posible tratando de preservar la originalidad de la prueba y en lo posible obteniendo copias de respaldo.

- Proceso Auditable

  Los procedimientos seguidos y la documentación generada deben haber sido válidos y contrastados por las buenas prácticas profesionales.

- Proceso reproducible

  Los métodos y procedimientos aplicados deben ser reproducibles, verificables y argumentables al nivel de comprensión de los entendidos en la materia, quienes puedan dar validez y respaldo a las actuaciones realizadas.

#### 2.3.3.2.3 Norma - ISO/IEC 27042: 2015

> "Esta Norma Internacional, pretende complementar otras normas y documentos que dan orientación sobre la investigación y la preparación para investigar incidentes de seguridad de la información. No es un guía completa, pero establece ciertos principios fundamentales destinados a garantizar que las herramientas, las técnicas y los métodos pueden seleccionarse adecuadamente y demostrarse que son aptos para el propósito en caso de que surja la necesidad. Tiene la intención de informar a los tomadores de decisiones que necesitan determinar la confiabilidad de la evidencia digital que se les presenta. Es aplicable a las organizaciones que necesitan proteger, analizar y presentar evidencia digital potencial. Es relevante para los órganos de formulación de políticas que crean y evaluar los procedimientos relacionados con la evidencia digital, a menudo como parte de un cuerpo de evidencia más grande" (ISO/IEC, 2015).

(International Standart, 2015) describe parte de un proceso de investigación integral que incluye, pero no se limita a las siguientes áreas temáticas:

- Gestión de incidentes, incluida la preparación y planificación de las investigaciones.
- Manejo de evidencia digital.
- Uso y problemas causados por la redacción.

- Sistemas de prevención y detección de intrusos, incluida la información que puede obtenerse de estos sistemas.
- Seguridad del almacenamiento, incluida la higienización del almacenamiento.
- Asegurar que los métodos de investigación sean adecuados para su propósito.
- Llevar a cabo análisis e interpretación de evidencia digital.
- Comprensión de los principios y procesos de las investigaciones de pruebas digitales.
- Gestión de eventos de incidentes de seguridad, incluida la derivación de evidencia de los sistemas involucrados en gestión de eventos de incidentes de seguridad.
- Relación entre el descubrimiento electrónico y otros métodos de investigación, así como el uso de técnicas de descubrimiento electrónico en otras investigaciones.
- Gobernanza de las investigaciones, incluidas las investigaciones forenses. Estas áreas temáticas se abordan, en parte, en las siguiente Norma ISO/CEI 27037.

En tal virtud unifica una serie de buenas prácticas acerca de la orientación sobre el análisis y la interpretación de las evidencias digitales, así como proporciona directrices sobre cómo el perito informático debe plantear el análisis e interpretación de la evidencia digital en un incidente o en una intervención pericial, desde la identificación (evidencia digital potencial), por consiguiente el análisis (evidencia digital) y por último la presentación y aceptación como prueba en un juicio (evidencia digital legal).

(GlobátiKa Peritos Informáticos, 2014) dentro de la información que el perito informático puede incluir en su informe pericial, se enumera las siguientes:

- ✓ Calificaciones del perito informático.

- ✓ Información inicial de que se dispone del perito informático y su equipo.
- ✓ Naturaleza del incidente que va a ser investigado por el perito informático.
- ✓ Fecha, hora y duración del incidente.
- ✓ Lugar del incidente.
- ✓ Objetivos de la investigación.
- ✓ Miembros del equipo de investigación supervisados por el perito informático.
- ✓ Fecha, hora y duración de la investigación.
- ✓ Lugar de la investigación.
- ✓ Hechos sustentados por una evidencia digital y hallados durante la investigación.
- ✓ Daños en la evidencia digital y sus implicaciones en los siguientes estadios del proceso de investigación.
- ✓ Limitaciones de todos los análisis realizados.
- ✓ Detalle del proceso y herramientas utilizadas.
- ✓ Interpretación de la evidencia digital por parte del perito informático.
- ✓ Conclusiones.
- ✓ Recomendaciones.

#### 2.3.3.3 Preservación de la evidencia digital.

Se documenta el cómo ha sido preservada la evidencia, es imprescindible definir los métodos adecuados para el almacenamiento y etiquetado de las evidencias. Una vez que se cuente con todas las evidencias del incidente se requiere conservarlas intactas, ya que son “huellas del crimen” y como tal se debe asegurar la correcta aplicación de la cadena de custodia. Aquí es donde se fijarán las responsabilidades y controles del personal técnico que manipule la evidencia digital; se precisa la elaboración de un registro donde consten

los datos como: nombres, fechas, custodios, lugar de almacenaje, transporte, etc.

**Figura 2.3.3.3.1:** Preservación de la evidencia digital.
**Fuente:** (Pinto, 2014).

### 2.3.3.4 Análisis de la evidencia digital.

Posteriormente a que se haya realizado los procesos de identificación, recopilación y preservación de las evidencias digitales, se prepara las herramientas y técnicas que se pondrán de manifiesto en el desarrollo del análisis forense, cuyo fin prioritario es reconstruir con todos los datos disponibles la cadena de acontecimientos en la que se llevó a cabo el incidente.

**Figura 2.3.3.4.1:** Análisis de la evidencia digital.
**Fuente:** (Pinto, 2014).

Este análisis deberá responder las preguntas de cómo se llevó a cabo el incidente, por quién o quienes fue realizado, en qué circunstancias se llevó a cabo, el objetivo de incidente e identificar los daños causados.

Para la realización del análisis forense de las evidencias digitales, existen herramientas informáticas tales como:

- Encase.- software de investigación forense informático, que tiene la capacidad de realizar el análisis complejo de la evidencia digital en diversas plataformas.

  - ✓ Amplia compatibilidad de formatos disponibles.
  - ✓ Amplia compatibilidad con navegadores.
  - ✓ Análisis y generación de informes de manera detallada.
  - ✓ Recopilación inteligente de evidencia digital.

- FTK Imager.- potente herramienta forense enfocada básicamente a la adquisición y tratamiento de las imágenes de cualquier dispositivo de almacenamiento, para ser posteriormente usadas como evidencias forenses en un proceso legal.

  - ✓ Volcado de la memoria RAM
  - ✓ Interfaz intuitiva
  - ✓ Potente velocidad de procesamiento
  - ✓ Creación de imágenes bit a bit de discos duros y demás unidades de almacenamiento.
  - ✓ Creación de hashes de archivos y dispositivos (md5 y sha1) – prueba de que los ficheros no han sido alterados, ni modificado en ningún caso.

- Digital Forensics Framework .- herramienta basada en Python con un módulo de sistema flexible para investigación forense digital de memorias USB, PDA, tarjetas de memoria y celulares.

  - ✓ Recuperación potente de archivos borrados.

- ✓ Análisis del sistema de archivos de teléfonos móviles.
- ✓ Descifrar contenido y metadatos de SMS para mostrarlos como en un teléfono móvil.

- Easy Recovery Professional.- Es una solución para recuperar datos, recuperar archivos, correo electrónico y realizar diagnóstico de discos.

  - ✓ Discos duros IDE/ATA/SATA/SCSI
  - ✓ Discos extraíbles
  - ✓ Soportes periféricos
  - ✓ Soportes digitales

Las herramientas antes mencionadas deben contar con licenciamiento profesional.

### 2.3.3.5 Documentación y Resultados.

El investigador, debe asegurar que todas las fases que intervinieron en el desarrollo del análisis forense se documentaron correctamente, está acción le permite gestionar el incidente, llevando un mejor control de los procedimiento o mecanismos ejecutados de principio a fin del proceso de análisis.

Para un correcto y eficaz registro de los procedimientos realizados se sugiere mantener los siguientes formularios:

- Formulario para el control de custodia de evidencias.
- Formulario de identificación de equipos y componentes.
- Formulario de incidencias tipificadas.
- Formulario de publicación del incidente.
- Formulario de recogida de evidencias.
- Formulario de discos duros.

En está, se elabora los informes técnicos, que contienen una declaración pormenorizada del análisis efectuado, metodología, técnicas y el compendio de los hallazgos encontrados.

#### 2.3.3.5.1 Informe Técnico.

Este informe consiste en una exposición detallada del análisis efectuado describe a profundidad la metodología, técnicas y hallazgos del equipo forense.

El informe técnico por lo menos debe contener los siguientes aspectos técnicos:

a. Antecedente del incidente
   - ✓ Recolección de los datos.
   - ✓ Descripción de la evidencia.
   - ✓ Entorno del análisis.

b. Descripción de las herramientas
   - ✓ Análisis de la evidencia.

c. Información del sistema
   - ✓ Características del SO.
   - ✓ Aplicaciones.
   - ✓ Servicios.
   - ✓ Vulnerabilidades.
   - ✓ Metodología.

d. Descripción de los hallazgos.
   - ✓ Huellas de la instrucción.
   - ✓ Herramientas usadas por el atacante.
   - ✓ Alcance de la intrusión.
   - ✓ El origen del ataque.

e. Cronología de la intrusión.
f. Conclusiones.
g. Recomendaciones específicas.
h. Referencias.

#### 2.3.3.5.2 Informe Ejecutivo.

Consiste en un resumen del análisis realizado, empleando un lenguaje no técnico, donde se expondrá los hechos más destacables de lo ocurrido en el sistema analizado. Es aconsejable que el mencionado informe contenga entre tres y cinco páginas, de lo actuado, en razón que la información que se detalle se expondrá a personal no especializado.

El informe ejecutivo debe contener los siguientes ítems:

a. Desarrollo de la intrusión.
b. Resultados del análisis.
c. Recomendaciones.

# CAPÍTULO III

# “DEL INFORME TÉCNICO PERICIAL INFORMÁTICO”

## 3.1 Peritaje informático.

El dictamen pericial define como, una actividad procesal mediante la que una persona o institución especialmente calificada suministra al juez argumentos o razones para la formación de su convencimiento acerca de ciertos datos controvertidos, cuya percepción o comprensión escapa a las aptitudes comunes judiciales (Gimeno Sendra, 2010).

En su libro de Derecho Procesal Penal, Colín Sánchez (2010) define al dictamen pericial como, el acto procedimental en el que el técnico o especialista en una arte o ciencia (perito), previo examen de una persona, de una conducta o hecho, o cosa, emite un dictamen conteniendo su parecer y los razonamientos técnicos sobre la materia en la que ha pedido su intervención.

Por consiguiente, si bien es cierto los magistrados son profesionales de justicia, ellos no cuentan con los conocimientos y destrezas técnicas informáticas, que puedan ser aplicados en la solución de un caso judicial, por lo que recurren a la prueba pericial, solicitando la colaboración de expertos en la materia a investigar, a fin de que entreguen su pronunciamiento al respecto de las evidencias encontradas, las cuales pueden estar relacionadas con el origen o procedencia del evento o suceso actuado. En este sentido, el peritaje informático se caracteriza por proporcionar a los magistrados, argumentos o razones acerca de los aspectos que resulten controvertidos en una determinada situación técnica informática y además tenga relevancia jurídica.

Siendo que la obtención de evidencias digitales se logra mediante la realización de un análisis, supone una actividad compleja que se ha tratado de estandarizar sin mucho éxito a lo largo de los últimos 20 años. Han sido muchas las propuestas realizadas a nivel internacional, intentando hacer frente al continuo crecimiento y diversidad de los delitos informáticos, para desarrollar una metodología que permita

definir un marco de actuación estándar y que tenga la consistencia necesaria para llevar a cabo una investigación forense de sistemas de información o dispositivos tecnológicos. No existe un consenso para elegir ninguno de estos marcos en concreto, debido a que cada metodología propuesta tiene sus ventajas e inconvenientes.

No obstante, las diferencias entre ellas no son absolutas, consistiendo en ocasiones simplemente en diferencias de denominación de los diversos pasos o actividades que integran el modelo de realización del análisis forense o en aglutinar algunos de ellos, comenzando con la identificación del incidente y la preparación de su análisis dentro de una estrategia de aproximación al mismo, siguiendo con la preservación y recopilación de las evidencias digitales para el examen y el análisis, y por último la presentación de los resultados obtenidos de forma que se dote al informe de rigor y consistencia, que son requisitos necesarios para hacerle frente a una posible impugnación (García, 2015).

Por otra parte, para lograr la convicción del juez frente a la prueba pericial presentada, tan importante como elaborar un buen informe pericial, es garantizar que las evidencias digitales encontradas han sido almacenadas de forma segura y sin posibilidad de alteración o que se haya mantenido la cadena de custodia, definida como el proceso utilizado para documentar la historia cronológica de un medio de prueba digital, con el objetivo de convencer al tribunal de que es razonablemente probable que la exposición sea auténtica así como de que nadie ha alterado dicho medio de prueba (Álvarez, R., Climent, J. J., Ferrández Agulló, F., Martínez Pérez, F. M., Tortosa, L., Vicent, J. F., & Zamora, A., 2014).

La garantía básica de inalterabilidad se documenta y consigue mediante la huella digital o función hash obtenida de cada evidencia digital, de manera que siempre se pueda comprobar a posteriori el hash original. Adicionalmente, para probar la historia cronológica de la cadena de custodia de una evidencia digital, será necesaria la constancia documentada acerca de cómo se ha manejado dicha evidencia a lo largo del tiempo, es decir, de “quién, qué, cuándo, dónde y, por qué ha manejado, para lo que se han propuesto algunos modelos de referencia metodológicos (García, 2015)(Jasmin & Miroslav, 2010).

### 3.3.1 Importancia de la pericia.

Las nuevas tecnologías y los dispositivos electrónicos son una de las vulnerabilidades a las que estamos expuestos a la hora del cometimiento de los delitos informáticos y es precisamente por esa razón que hoy en día las pruebas digitales, electrónicas y virtuales son una pieza clave en los procesos judiciales.

Gimeno Sendra (2010) destaca que el dictamen de peritos, informe pericial o peritaje como se suele denominar, es considerado, en la práctica del proceso civil el medio de prueba de mayor relevancia junto con la prueba documental.

Adquiere mayor importancia cuando en la controversia intervienen aspectos técnicos de tipo informático, debido a la necesidad, ineludible en la mayor parte de las ocasiones, de aportar de manera inteligible los conocimientos técnicos específicos al caso que faciliten al juez la formación de convicción. Así mismo, resulta relevante destacar que los peritajes informáticos no solo sirven como medio de prueba en los distintos procesos judiciales o discusiones extrajudiciales, en donde su uso es solicitado por los intervinientes con la finalidad de alcanzar una solución acerca de los elementos controvertidos o también como paso preliminar para iniciar un posterior proceso judicial (García, 2015).

### 3.3.2 Prueba valor probatorio.

(Palacio, 2000) concibe a la prueba como el conjunto de actos procesales, cumplidos con el auxilio de los medios previstos o implícitamente autorizados por la ley, y encaminados a generar la convicción judicial acerca de la existencia o inexistencia, la veracidad o la falsedad, de los hechos sobre los cuales versa la imputación.

Según Gómez del Castillo (2000 - 2001) prueba es una actividad (y un resultado) de acreditación o convencimiento de la verdad o certeza de un determinado hecho: La prueba implica así, un objetivo intelectual que se alcanza mediante percepciones sensitivas (fundamentalmente la vista y el oído, pero

también el olfato, el gusto y el tacto) que nos proporcionan personas o cosas (lo que las personas dicen o escriben y lo que las cosas muestran o enseñan), en cuanto a fuentes, materias o instrumentos probatorios.

Siendo así, las sentencias judiciales deben fundamentarse en las disposiciones legales y en los méritos del proceso, siendo primordial en este último aspecto la prueba aportada por las partes en orden a la justificación de sus aseveraciones. En el ámbito penal lo manifestado cobra mayor importancia, tomando en consideración que los hechos delictivos son perpetrados con la intención de no dejar huella o señales aparentes por parte de quien los comete.

En tal virtud es imprescindible establecerse y comprobarse dentro del proceso penal tanto la existencia de la infracción como la culpabilidad de los acusados, entrando en juego por ende la relevancia de la prueba y los medios probatorios, en procura de obtener aquellos elementos de cargo y descargo que permitan sustentar una acusación o desestimar las imputaciones que se formulen (Vayas Freire, 2009).

En consecuencia, los indicios encontrados en el desarrollo de la investigación de un proceso penal se los establece como pruebas, cuyo propósito es determinar los hechos que intervinieron en la comisión de un delito, así como precisar la responsabilidad del procesado en el grado de autor, cómplice, encubridor o se ratifique su inocencia.

#### 3.3.2.1 Prueba electrónica.

Marval Victor (2010) señala que la prueba electrónica, podría encontrar su lugar en la regulación de la prueba documental ya que la noción de documento ha evolucionado de forma flexible superando su tradicional aceptación como escrito, con la finalidad de proporcionar cobijo y cobertura a los nuevos medios probatorios proporcionados por la aplicación de nuevas tecnologías para la presentación de la realidad. De esta manera se le proporcionaría toda la protección inherente a esta prueba en orden a su puesta en práctica (traslado a las partes en el acto del juicio para su examen,

práctica anticipada y diligencias para mejor proveer, etc.), o como llave que abre el acceso a recursos como el de suplicación.

La prueba electrónica es aquella información obtenida a través de un dispositivo electrónico o medio digital, el cual sirve para adquirir convencimiento de la certeza de un hecho en un juicio (Mérida, 2008).

### 3.2 Peritaje informático.

Con la ayuda de la informática forense se puede autentificar las pruebas en los dispositivos digitales: a) correos electrónicos; b) agendas electrónicas; c) teléfonos celulares; d) grabaciones de voz con análisis de sonografía y espectrografía; e) nóminas digitales; f) computadoras portátiles; g) pago por medios electrónicos; h) correo fotográfico, etc.

En opinión del perito en informática forense (Velázquez A, 2000) los examinadores forenses digitales, son profesionales que cuentan con conocimientos de los fenómenos técnicos en informática; se encuentran preparados para aplicar procedimientos técnicamente válidos, conocimiento del proceso de inteligencia y entendimiento del marco legal para obtener la evidencia en situaciones donde se vulneran/comprometan los sistemas informáticos.

Comenta que en algunos casos esta investigación será para uso interno; en otras, como elemento de prueba, donde la computadora se haya usado como medio para cometer algún delito. Una de las tareas del perito en informática forense inicialmente es congelar la evidencia y asegurarla, para posteriormente presentarla en su análisis. El aseguramiento se hace única y exclusivamente mediante la utilización de herramientas de software y hardware, que a su vez utilizan métodos matemáticos complejos para copiar cada medio magnético en forma idéntica; es decir, que les permita obtener copias digitales idénticas al original.

El perito define a la informática forense como la aplicación de técnicas científicas y analíticas especializadas a la infraestructura tecnológica que permiten identificar; preservar, analizar y presentar datos que sean válidos dentro de un proceso judicial.

Dichas técnicas incluyen al reconstruir el bien informático, examinar datos residuales, autentificar datos y bienes informáticos.

El perito ejemplifica un ejercicio pericial: antes de analizar de hecho, el investigador debe inmediatamente generar una imagen forense de todo el contenido del dispositivo, incluyendo el espacio libre.

El perito una vez que se ha cumplido apropiadamente con el aseguramiento de la evidencia, además de congelar la misma y generar la imagen digital, deberá preservar la evidencia, según el caso, para que la información no pueda ser manipulada (Velázquez A, 2000).

### 3.2.1 Normativa relacionada con el peritaje informático.

El peritaje informático se encuentra regulado por la normativa procesal correspondiente a la prueba pericial establecida, dentro de los diversos órdenes jurisdiccionales. No existe, por tanto, ninguna especialidad en el tratamiento normativo dado a la pericia informática respecto al del resto de pericias. De esta manera, es posible decir que el peritaje informático es, desde el punto de vista de su tratamiento procesal, un peritaje más, así el momento y la forma de aportación del dictamen pericial al proceso, su valoración por el juez, las obligaciones y las condiciones del perito, su posible tacha o recusación o posible actuación en el juicio, se rigen por las mismas reglas que cualquier otro tipo de peritaje (García, 2015).

Así, en la constitución del Ecuador se tiene las siguientes normas procesales aplicables para el desarrollo de la pericia:

| **Sección Tercera – Etapa de Juicio**<br>**Párrafo primero – Instalación** | |
|---|---|
| **Art. 611.-** Notificaciones | • La o el juzgador notificará a los testigos o peritos para su comparecencia a la audiencia, siendo responsabilidad de los sujetos procesales el llevar dichos peritos o testigos a la misma. |

| Párrafo Segundo – Práctica de pruebas | |
|---|---|
| **Art. 615.-** Práctica de Pruebas. | • Los peritos deberán exponer el contenido de las conclusiones de su informe y a continuación se autorizará interrogarlos. |

**Tabla 3.2.1.1:** Normativa en relación a la pericia.

**Fuente:** (Asamblea Nacional, COIP, 2014)**.**

En tal virtud, los jueces son los únicos responsables de designar y ordenar a los peritos que practiquen las diligencias y actuaciones necesarias para dilucidar un proceso investigativo.

### 3.2.1.1 Obligaciones de los peritos informáticos en Ecuador.

Capítulo IV Obligaciones de los peritos: **Art. 18.- Obligaciones Generales** (Judicatura, 2016)**:**

- Desempeñarán su función con objetividad, imparcialidad, responsabilidad, oportunidad, puntualidad, rectitud, corrección y honestidad, enmarcado en todo momento en la ética, con la presentación de su criterio técnico y especializado, exento de juicios de valor de ningún tipo.

- 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 **Art. 19.- Obligaciones específicas de los peritos**, 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.

- Presentar el informe correspondiente, de forma verbal y/o escrita, según lo que la normativa procesal establezca, con los requisitos mínimos establecidos en este reglamento y la ley; y, subirlo al Sistema Informático Pericial, en archivo tipo PDF.
- Presentar obligatoriamente y dentro del plazo otorgado, las aclaraciones, ampliaciones o complementos al informe presentado que ordene la autoridad judicial competente.
- Explicar y defender el informe presentado, sus conclusiones en las audiencias orales de prueba o de juicio para las cuales fuere notificado legalmente, si la ley así lo prevé.
- Presentar la copia certificada de la factura de honorarios emitida por su persona, por el trabajo pericial realizado;
- Aprobar los cursos de capacitación determinados en el presente reglamento. y;
- Cualquier otra obligación establecida en la normativa legal, en este reglamento y/o por la o el administrador del sistema pericial.

### 3.2.2 Servicios de los peritos informáticos.

Según (Group Blog Especialidades Perito Judicial, 2022) los servicios más demandados de los Peritos Judiciales Informáticos son los siguientes:

- **Extracción de datos de móvil o WhatsApp,** se trata de certificar el contenido del móvil, de mensajes recibidos, vídeos o audios, de cara a utilizarlos como prueba en un procedimiento judicial.

- **Análisis de Discos y recuperación de datos,** el perito realiza un análisis de dispositivos de almacenamiento (discos duros, estaciones de trabajo, servidores, portátiles, sobremesa, etc), con el fin de identificar datos borrados, analizar el robo de datos, y detectando infracciones de propiedad intelectual.

- **Correo electrónico y medios de comunicación informáticos,** la verificación de correos electrónicos es una de las principales labores de los

informáticos forenses, autentificando que no han sido alterados o falsificados. Así como recuperando los mensajes borrados de los servidores, dispositivos de almacenamiento, tablets, móviles, etc.

- **Análisis de Smartphones, Tablets y dispositivos móviles**, como hemos dicho, el análisis forense de smartphones, tablets y otros dispositivos portátiles, puede dar lugar a conseguir una prueba fundamental e irrefutable para el caso. Estos trabajos pueden incluir la recuperación de mensajes borrados, registros de llamadas, documentos, e incluso geolocalización en un momento determinado.

- **Descubrimiento electrónico forenses base de datos,** el análisis y recuperación de datos en los diferentes sistemas operativos permite comprobar los documentos en un momento dado, así como su contenido.

- **Informático Forense en otros dispositivos digitales,** se refiere a la extracción de datos de unidades de GPS, sistemas informáticos de vehículos, coches autónomos, consolas de videojuegos, reproductores MP3, memorias USB, tarjetas SD, etc.

- **La preparación de peritaciones informáticas,** el estudio y análisis forense de medios informáticos conlleva la planificación de procedimientos, llevar a cabo la investigación, extracción de conclusiones y realización del informe pericial informático.

- **Sistemas de Protección DDoS,** análisis de sistemas de protección, vulnerabilidades, así como estudio de ataques.

- **Seguridad informática, comprende** la prevención, medidas de seguridad, así como la detección y evaluación de ataque de las mismas.

### 3.3 Informe técnico pericial.

El perito informático documentará toda la información que se generó en las etapas previas, resaltando la información de relevancia para la toma de

decisiones del Juzgador o interesado en el caso investigado. Se debe detallar una línea de los eventos que sucedieron con la evidencia y registrarlos, sustentándolos con los procesos aplicados.

El informe pericial como característica especial debe ser redactado de forma que sea fácil de entender pensando que quién lo va a leer no son técnicos, pero debe contener el sustento de los resultados obtenidos.

En el informe pericial, la evidencia debe ser adjuntada; considerando que cuando la evidencia sea presentada debe contener métodos para permitir únicamente la lectura, en el desarrollo del informe se debe tomar en cuenta las siguientes actividades:

- Durante el proceso de identificación, recolección, adquisición y preservación de la evidencia ningún detalle debe dejarse fuera.
- El Investigador debe considerar que el formato fecha y hora se encuentren sincronizados con una fecha válida a fin de registrar en el informe.
- Registrar todo lo que puede visualizar por el monitor o pantalla del dispositivo por ejemplo programas activos, procesos, nombres de documentos abiertos, capturas que deben registrarse con una breve descripción.
- Cualquier operación realizada con el operador debe ser registrada.

Según el (Judicatura, 2016) los requisitos mínimos obligatorios de todo informe pericial son los siguientes:

| **Contenido del Informe Pericial - Capítulo V** | |
|---|---|
| **Art. 21.-** Informe Pericial | • **Parte de antecedentes**, en donde se debe delimitar el objeto del peritaje, esto es, se tiene que especificar claramente el tema sobre el que informará en base a lo ordenado por la jueza o juez, la o el fiscal y/o lo solicitado por las partes procesales. |

| Contenido del Informe Pericial - Capítulo V | |
|---|---|
| | • **Parte de consideraciones técnicas o metodología a aplicarse,** en donde se debe explicar claramente como aplican sus conocimientos especializados de una profesión, arte u oficio al caso o encargo materia de la pericia.<br>• **Parte de conclusiones**, luego de las consideraciones técnicas, se procederá a emitir la opinión técnica, o conclusión de la aplicación de los conocimientos especializados sobre el caso concreto analizado. La conclusión será clara y directa en relación a la pericia realizada. Se prohíbe todo tipo de juicios ambiguos, así como cualquier tipo de juicio de valor, sobre la actuación de las partes en el informe técnico; y<br>• **Parte de Inclusión de documentos de respaldo, anexos, o explicación de criterios técnicos**, deberá sustentar sus conclusiones ya sea con documentos y objetos de respaldo (fotos, láminas demostrativas, copias certificadas de documentos, grabaciones de audio y video, etc.) y/o, con la explicación clara de cuál es el sustento técnico o científico para obtener un resultado o conclusión específica. Se debe exponer claramente las razones especializadas del perito para llegar a la conclusión correspondiente. No se cumplirá con este requisito si no se sustenta la conclusión con documentos, objetos, o con la explicación técnica y científica exigida en este numeral.<br>Formato Modelo de Informe Pericial (ANEXO – B) |

**Tabla 3.3.1:** Contenido del Informe Pericial.

**Fuente:** (Reglamento del Sistema Pericial Integral de la Función Judicial, 2016).

Por consiguiente y en relación al modelo de informe técnico pericial, Jaramillo Montoya Paula, en su trabajo de investigación presenta 103 informes provenientes del Consejo de la Judicatura, donde se evidencia que la organización no proporciona o estandariza las herramientas que deben ser

usadas por los peritos del área. Es decir, cada profesional debe realizar la pericia con los recursos disponibles (Jaramillo Montoya, 2019). (ANEXO – C)

# CAPÍTULO IV

# CONCLUSIONES Y RECOMENDACIONES

## 4.1 CONCLUSIONES

Del análisis realizado en el presente trabajo, se extraen las siguientes conclusiones:

- Una correcta y adecuada gestión de la evidencia digital, es fundamental en los procesos judiciales, ya que pone en manifiesto la exigente labor que se requiere por parte de los investigadores en la informática forense, los cuales deben aplicar procedimientos, técnicas y herramientas para obtener, custodiar, revisar, analizar y presentar la evidencia encontrada ante el tribunal, trasparentando una correcta cadena de custodia.

- Los pasos para el manejo de la evidencia digital en cuanto al registro, admisibilidad, valor probatorio, preservación, transformación y recuperación, deberá desprenderse de un manual de buenas prácticas en computación forense, teniendo especial cuidado en el documentando las acciones realizadas y justificando todas las decisiones aplicadas en las etapas del proceso.

- El perito informático debe documentar toda la información que se generó en las etapas previas, resaltando la información de relevancia para la toma de decisiones del Juzgador o interesado en el caso investigado, detallando una línea de los eventos que sucedieron con la evidencia y registrarlos, sustentándolos con los procesos aplicados.

- Los peritajes informáticos no solo sirven como medio de prueba en los distintos procesos judiciales o discusiones extrajudiciales, en donde su uso es solicitado por los intervinientes con la finalidad de alcanzar una solución acerca de los elementos controvertidos o también como paso preliminar para iniciar un posterior proceso judicial, adquieren mayor importancia cuando en la controversia intervienen aspectos técnicos de tipo informático, debido a la

necesidad, ineludible en la mayor parte de las ocasiones, de aportar de manera inteligible los conocimientos técnicos específicos al caso que faciliten al juez la formación de convicción.

## 4.2 RECOMENDACIONES

Al verificar la estructura del informe pericial, definida por el Consejo de la Judicatura se evidencia que la entidad no proporciona o estandariza las herramientas que deben ser usadas por los peritos para desarrollo del mismo, es decir cada profesional al realizar una pericia debe hacerlo con los recursos que tenga disponible, siendo que el objetivo del trabajo de investigación es: identificar las técnicas y metodologías empleadas para la elaboración del informe técnico pericial informático acorde a las Guías y Normas Internacionales, así como conocer las herramientas utilizadas tanto por los infractores como por los investigadores, se recomienda que el perito forense informático, efectué los siguientes pasos en el momento de elaborar el informe técnico pericial informático.

| Ord. | Actividad | Aplicar – Guía/ Norma |
|---|---|---|
| 1 | Ubicar la identidad de la agencia/departamento/unidad y peritos (s) que intervinieron en el análisis forense | Guía DoJ 2<br>Examen forense digital |
| 2 | Ubicar el número identificador del caso investigado (número de causa/proceso), la fecha de recepción del caso y la fecha del informe. | Guía DoJ 2<br>Examen forense digital |
| 3 | 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 |
| 4 | Detallar la información general de los dispositivos o equipos analizados, marca, modelo, serie etc. | Guía DoJ 2<br>Examen forense digital |

| | | |
|---|---|---|
| 5 | Describir brevemente las medidas adoptadas durante el examen (búsquedas de cadenas, búsquedas de imágenes, gráficos y recuperar archivos borrados) | Guía DoJ 2<br>Examen forense digital |
| 6 | Describir los programas y herramientas utilizados en el análisis de la evidencia | Guía DoJ 2<br>Examen forense digital |
| 7 | Detallar las técnicas y procedimientos utilizados en el análisis de la evidencia. | Guía DoJ 2<br>Examen forense digital |
| 8 | Determinar los resultados y conclusiones del caso investigado. | Guía DoJ 2<br>Examen forense digital |
| 9 | Incluir las limitaciones del análisis realizado. | ISO/IEC 27042 |

## BIBLIOGRAFÍA

### Direcciones Electrónicas


- Acurio del Pino Santiago, Manual de Manejo de Evidencias Digitales y Entornos Informáticos, Versión 2.0, Ecuador, (2009).
  Disponible en internet:
  https://www.oas.org/juridico/english/cyb_pan_manual.pdf
  Consultado el 30 marzo del 2022.

- Análisis normativo y jurisprudencial del peritaje informático, Blog de JL Abogadoteleco, blog jurídico-técnico sobre las TIC.
  Disponible en internet:
  http://blog.abogadoteleco.es/autor/
  Consultado el 17 de marzo del 2022.

- Andrés Velázquez, examinador forense digital, (29 de mayo del año 2000) Derecho Procesal Informático, profesor de informática forense del ITAM, campus Santa Teresa, diplomado “El marco legal de las tecnologías de la información”.
  Disponible en internet:
  https://pdfcoffee.com/derecho-procesal-informatico-4-pdf-free.html
  Consultado el 23 de marzo del 2022.

- Ariza, M y Quesada A. (2014), Nuevas tecnologías y aprendizaje significativo de las ciencias, (Ariza et al.., 2009), España.
  Disponible en internet:
  https://es.scribd.com/document/510685645/Ariza-Et-Al-Nuevas-Tecnologias-y-Aprendizaje
  Consultado el 17 de marzo del 2022.

- Asamblea Nacional Constituyente, Código Orgánico Penal, Registro Oficial Suplemento No. 180, 10 de febrero de 2014.
  Disponible en internet:
  https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/ECU/INT_CEDAW_ARL_ECU_18950_S.pdf
  Consultado el 16 de abril del 2022

- Bernal, J. S., (2015), Instrumento de Ratificación del Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, hecho en Estrasburgo el 28 de enero de 2003. AIS: Ars Iuris Salmanticensis, 3(2), 228-230.
  Disponible en internet:
  https://revistas.usal.es/index.php/ais/article/download/14392/14773
  Consultado el 15 de abril del 2022.

- Carcelén, J. M. B., (2014), Delitos informáticos en el COIP. - Albán Gómez, Ernesto, Manual de Derecho Penal Ecuatoriano – COIP, Ediciones legales, Primera Edición. Quito.
  Disponible en internet:
  https://www.cortenacional.gob.ec/cnj/images/pdf/publicaciones_cnj/Temas%20Penales%203.pdf#page=32
  Consultado el 15 de abril del 2022.

- Calderón, Frankz Alberto Carrera, Martínez, Mario Ramiro Aguilar, 2020, Guía integral de empleo de la informática forense en el proceso penal de Ecuador, Guía integral de empleo de la informática forense en el proceso penal de Ecuador, Universidad y Sociedad, vol. 12.
  Disponible en internet:
  https://rus.ucf.edu.cu/index.php/rus/article/download/1773/1771
  Consultado el 15 de abril del 2022

- Cobarrubias Vladimir, Ciencia Informática Forense, 27 de abril 2008, Santiago, Chile.
  Disponible en internet:
  https://forenseinformatico.blogspot.com/2008/04/
  Consultado el 17 de marzo del 2022.

- Constitución de la República del Ecuador, Asamblea Nacional Constituyente, Registro Oficial 449, 20 de octubre de 2008.
  Disponible en internet:
  https://www.superbancos.gob.ec/bancos/wp-content/uploads/downloads/2021/11/constitucion_republica_ecuador4.pdf
  Consultado el 15 de abril del 2022.

- Constitución de la República del Ecuador, Asamblea Nacional Constituyente, Registro Oficial Suplemento 180, 10 febrero 2014,
  Disponible en internet:
  https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/ECU/INT_CEDAW_ARL_ECU_18950_S.pdf
  Consultado el 15 de abril del 2022.

- Constitución de la República del Ecuador, Asamblea Nacional Constituyente, Registro Oficial Suplemento 585, 11 de septiembre 2015.
  Disponible en internet:
  https://www.cienciasforenses.gob.ec/wp-content/uploads/2017/08/DECRETO-EJECUTIVO-759-2015.pdf
  Consultado el 15 de abril del 2022.

- Convenio de Ciberdelincuencia del Consejo de Europa, (2007), The convenntion on Cybercrime. Budapest, capital territorial Hungría.
  Disponible en internet:
  https://blog.uclm.es/cienciaspenales/files/2016/10/1.-CONVENIO-DEL-CONSEJO-DE-EUROPA-SOBRE-CIBERDELINCUENCIA.pdf
  Consultado el 15 de abril del 2022.

- DFRWS, Carrier, B. (2002), Taller de Investigación Digital Forense, celebrado por un grupo de expertos en el año 2002, Defining Digital Forensic Examination and Analysis Tools, 07 de agosto del 2002.
  Disponible en internet:
  https://dfrws.org/wp-content/uploads/2019/06/2002_USA_paper-defining_digital_forensic_examination_and_analysis_tools.pdf
  Consultado el 16 de abril del 2022.

- DFRW, (2001), A Road Map for Digital Forensic Research, New York. Disponible en:
  https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf
  Consultado el 16 de abril del 2022.

- Espinoza Villamar, Jaime Jonathan; Verdezoto Acuña, Rómulo Gabriel, (2015), El rol de la auditoría forense ante los nuevos delitos informáticos tipificados en el actual código orgánico integral penal del Ecuador COIP, metodologías y herramientas a usar ante una evidencia digital.
  Disponible en internet:
  https://dspace.ups.edu.ec/handle/123456789/10348
  Consultado el 30 marzo del 2022.

- Eloff, J.H.P., M. Kohn, M.S Olivier, (2008), Information and computer security architectures (ICSA). Research Group. Department of Computer Science, University of Pretoria, South Africa.
  Disponible en internet:
  http://icsa.cs.up.ac.za/issa/2008/Proceedings/Full/25.pdf.
  Consultado el 16 de abril del 2022.

- Fiscalía General del Estado, Reglamento del Sistema Especializado Integral de Investigación, de medicina legal y ciencias forenses,1 de abril del 2014.
  Disponible en internet:
  https://www.fiscalia.gob.ec/transparencia/2018/septiembre/a3/literal_a3_regulaciones_y_procedimientos_resolucion_030_2014.pdf
  Consultado el 16 de abril del 2022.

- Fiscalía General del Ecuador, Resolución No. 073-FGE-2014 Manuales, Protocolos, Instructivos y Formatos del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses, Registro Oficial Suplemento No. 318, 25 de agosto 2014.
  Disponible en internet:
  https://www.cienciasforenses.gob.ec/wp-content/uploads/downloads/2017/10/registro-oficial-318-MANUALES-PROTOCOLOS.pdf
  Consultado el 15 de abril del 2022.

- Globálika - Peritos Informáticos, (2014), El perito informático y el proceso judicial.
  Disponible en internet:
  https://peritosinformaticos.es/el-perito-informatico-y-el-proceso-judicial/
  Consultado el 17 de marzo del 2022.

- Globálika - Peritos Informáticos, (2014), ISO/IEC 27037:2012 y el Perito Informático.
  Disponible en internet:
  https://peritosinformaticos.es/que-es-un-perito-informatico-te-explicamos-su-labor/
  Consultado el 17 de marzo del 2022.

- ISO/IEC 27042 - International Standart, (2015), Information technology - Security techniques- Guidelines - for the analysis and interpretation of digital evidence.
  Disponible en internet:
  https://webstore.iec.ch/preview/info_isoiec27042%7Bed1.0%7Den.pdf
  Consultado el 30 de marzo del 2022.

- Jaramillo Montoya Paula Romina, junio 2019, 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.
  Disponible en internet:
  http://repositorio.puce.edu.ec/bitstream/handle/22000/17774/Romina_Jaramillo_Tabajo_de_Titulacion.pdf?sequence=1&isAllowed=y
  Consultado el 30 de marzo del 2022.

- López Delgado Miguel, Edición 2da -junio 2007, Análisis Forense Digital.
  Disponible en internet:
  https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf
  Consultado el 17 de marzo del 2022.

- NACIONES UNIDAS, Oficina contra la Droga y el Delito. Undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal.
  Disponible en internet:
  http://www.11uncongress.org
  Consultado el 21 de abril de 2022.

- NACIONES UNIDAS, Undécimo Congreso de las Naciones Unidas sobre prevención del Delito y Justicia - Delitos Informáticos, 25 de abril del 2005.
  Disponible en internet:
  http://www.unis.unvienna.org
  Consultado el 21 de abril de 2022.

- Pinto Diego, Maskana,I+D+ingeniería 2014, Metodología de análisis forense a incidentes en dispositivos móviles, 17 octubre 2014.
  Disponible en internet:
  https://publicaciones.ucuenca.edu.ec/ojs/index.php/maskana/article/download/721/641/2232
  Consultado el 15 de abril del 2022.

- SANS Institute InfoSec Reading Room, Ryder, K., (2002), Computer Forensics-We've Had an Incident, Who Do We Get to Investigate.
  Disponible en internet:
  https://www.sans.org/white-papers/652/
  Consultado el 15 de abril del 2022.

- Santos Tello, Jorge, Procedimientos en la investigación, recolección y manejo de la evidencia digital en la escena del crimen [En línea] Hueheutango, septiembre del 2013. [Citado en 28 marzo de 2016].
  Disponible en internet:
  http://biblio3.url.edu.gt/Tesario/2013/07/03/Santos-Jorge.pdf
  Consultado el 9 de abril de 2022.

- Vayas Freire, G. (2009), Medios probatorios admitidos en la legislación adjetiva penal del Ecuador (Master's thesis, Universidad Andina Simón Bolívar, Sede Ecuador), 03 de agosto del 2009.
  Disponible en internet:
  https://repositorio.uasb.edu.ec/bitstream/10644/689/1/T771-MDE-Vayas-Medios%20probatorios%20admiitidos%20en%20la%20legislaci%C3%B3n.pdf
  Consultado el 23 de abril del 2022.

**Libros**


- Álvarez, R., Climent, J. J., Ferrández Agulló, F., Martínez Pérez, F. M., Tortosa, L., Vicent, J. F., & Zamora, A., (2014), Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información, RECSI XIII, Alicante.
- Camacho Losa, L., (1987), El delito informático. Madrid, Gráficas Cóndor.
- Cano, J., (2009), Computación forense descubriendo los rastros informáticos en: Computación forense descubriendo los rastros informáticos, México, Editorial AlfaOmega.
- Casabona Romeo, Carlos María, (1987), Poder Informático y Seguridad Jurídica, Fundesco, Madrid, España.
- Colín Sánchez, Guillermo, (2010), Derecho mexicano de procedimientos penales, Editorial Porroua.
- Cosic, J., & Baca, M., (2010), A Framework to (Im) Prove" Chain of Custody" in Digital Investigation Process, In Central European Conference on Information and Intelligent Systems, Faculty of Organization and Informatics Varazdin.
- Domínguez, Francisco Lázaro. (2014), Introducción a la informática forense, Madrid, España, Grupo Editorial RA-MA.
- Gimeno Sendra José Vicente, (2010), Derecho Procesal Civil: El proceso de declaración, Parte General, Colex 2010. 3ª edición.
- Hoog, (2011), Android forensics: Investigation, analysis, and mobile security for Google Android, Syngress.
- Jeimy J. Cano M, (2006), Introducción a la informática Forense, revista sistemas N0 96, publicado por Asociación Colombiana de Ingeniero de Sistemas (ACIS).
- Larry, D., D. Lars, (2012), Digital forensics for legal professionals, understanding digital evidence from the warrant to the courtroom. Syngress, Waltham.
- Larry Daniel, Lars Daniel, (2012), Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom, 1st Edición, Syngress, Waltham.
- Lázaro, (2013), Introducción a la informática forense, España, RA-MA.

- Lima, María de la Luz Lima, (1984), Delitos Electrónicos, México, Ediciones Porroua.
- Mandia, K., C. Prosise, (2003), Incident response & computer forensics, 2a ed., McGraw-Hill.
- Mata y Martin, Ricardo, (1989), Delincuencia informática y derecho penal Definición adoptada en las conclusiones del congreso sobre “Delito Informático”, España, Zaragoza.
- Palacio, Lino Enrique, (2000), La prueba en el proceso penal, Buenos Aires, Abeledo, Perrot,
- Pinto, D. (2014), Metodología de análisis forense orientada a incidentes en dispositivos móviles, Maskana, 5.
- Prosise, C., Mandia, K., & Pepe, M., (2003), Incident response & computer forensics, Second Edition, New York, McGraw-Hill/Osborne.
- Téllez Valdés, Julio. (1996), Derecho Informático, 2da Edición, México, Editorial Mc Graw Hill.
- Reyes Anthony, (2007), Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement and Prosecutors, Editorial Amorette Pendersen, Estados Unidos.
- Tiedemann, Klaus. (1985), Poder económico y delito. Barcelona, Ariel.
- Watson, D. L. & Jones, A., (2013), Digital forensics processing and procedures: Meeting the requirements of ISO 17020, ISO 17025, ISO 27001 and best practice requirements, Newnes, Syngress, Waltham.

# ANEXO - A

## Guías existentes a nivel mundial de mejores prácticas en computación forense

**RFC 3227 - Guía Para Recolectar y Archivar Evidencia" (Guidelines for Evidence Collection and Archiving) [GuEvCo02]**, **escrito en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group.**

Es un documento que provee una guía de alto nivel para recolectar y archivar datos relacionados con intrusiones. Muestra las mejores prácticas para determinar la volatilidad de los datos, decidir que recolectar, desarrollar la recolección y determinar cómo almacenar y documentar los datos. También explica algunos conceptos relacionados a la parte legal.

Su estructura es:

a) Principios durante la recolección de evidencia: orden de volatilidad de los datos, cosas para evitar, consideraciones de privacidad y legales.
b) El proceso de recolección: transparencia y pasos de recolección.
c) El proceso de archivo: la cadena de custodia y donde y como archivar.

**Guía de la IOCE: La IOCE [IOCE06], publico "Guía para las mejores prácticas en el examen forense de tecnología digital" (Guidelines for the best practices in the forensic examination of digital technology) [IOCE02].**

El documento provee una serie de estándares, principios de calidad y aproximaciones para la detección prevención, recuperación, examinación y uso de la evidencia digital para fines forenses. Cubre los sistemas, procedimientos, personal, equipo y requerimientos de comodidad que se necesitan para todo el proceso forense de evidencia digital, desde examinar la escena del crimen hasta la presentación en la corte.

Su estructura es:

a) Garantía de calidad (enunciados generales de roles, requisitos y pruebas de aptitud del personal, documentación, herramientas y validación de las mismas y espacio de trabajo).
b) Determinación de los requisitos de examen del caso.

c) Principios generales que se aplican a la recuperación de la evidencia digital (recomendaciones generales, documentación y responsabilidad).
d) Prácticas aplicables al examen de la evidencia de digital.
e) Localización y recuperación de la evidencia de digital en la escena: precauciones, búsqueda en la escena, recolección de la evidencia y empaquetado, etiquetando y documentación.
f) Priorización de la evidencia.
g) Examinar la evidencia: protocolos de análisis y expedientes de caso.
h) Evaluación e interpretación de la evidencia
i) Presentación de resultados (informe escrito).
j) Revisión del archivo del caso: Revisión técnica y revisión administrativa.
k) Presentación oral de la evidencia.
l) Procedimientos de seguridad y quejas.

**Investigación en la Escena del Crimen Electrónico (Guía DoJ 1) El Departamento de Justicia de los Estados Unidos de América (DoJ EEUU), publico "Investigación En La Escena Del Crimen Electrónico" (Electronic Crime Scene Investigation: A Guide for First Responders) [ElCr01].**

Esta guía se enfoca más que todo en identificación y recolección de evidencia.
Su estructura es:

a) Dispositivos electrónicos (tipos de dispositivos se pueden encontrar y cuál puede ser la posible evidencia).
b) Herramientas para investigar y equipo.
c) Asegurar y evaluar la escena.
d) Documentar la escena.
e) Recolección de evidencia.
f) Empaque, transporte y almacenamiento de la evidencia.
g) Examen forense y clasificación de delitos.
h) Anexos (glosario, listas de recursos legales, listas de recursos técnicos y listas de recursos de entrenamiento).

**Examen Forense de Evidencia Digital (Guía DoJ 2) Otra guía del DoJ EEUU, es "Examen Forense de Evidencia Digital" (Forensic Examination of Digital Evidence: A Guide for Law Enforcement) [FoEx04].**

Esta guía está pensada para ser usada en el momento de examinar la evidencia digital.

Su estructura es:

a) Desarrollar políticas y procedimientos con el fin de darle un buen trato a la evidencia.
b) Determinar el curso de la evidencia a partir del alcance del caso.
c) Adquirir la evidencia.
d) Examinar la evidencia.
e) Documentación y reportes.
f) Anexos (casos de estudio, glosario, formatos, listas de recursos técnicos y listas de recursos de entrenamiento).

**Computación Forense - Parte 2: Mejores Prácticas (Guía Hong Kong) El ISFS, Information Security and Forensic Society (Sociedad de Seguridad Informatica y Forense) creada en Hong Kong, publico "Computación Forense - Parte 2: Mejores Prácticas" (Computer Forensics – Part 2: Best Practices) [CoFor04].**

Esta guía cubre los procedimientos y otros requerimientos necesarios involucrados en el proceso forense de evidencia digital, desde el examen de la escena del crimen hasta la presentación de los reportes en la corte.

Su estructura es:

a) Introducción a la computación forense.
b) Calidad en la computación forense.
c) Evidencia digital.
d) Recolección de Evidencia.
e) Consideraciones legales (orientado a la legislación de Hong Kong).
f) Anexos.

**Guía De Buenas Prácticas Para Evidencia Basada En Computadores (Guía Reino Unido) La ACPO, Association of Chief Police Officers (Asociación de Jefes de Policía), del Reino Unido mediante su departamento de crimen por computador, publico "Guía de Buenas Prácticas para Evidencia basada en Computadores" (Good Practice Guide For Computer Based Evidence) [GoPra99].**

La policía creó este documento con el fin de ser usado por sus miembros como una guía de buenas prácticas para ocuparse de computadores y de otros dispositivos electrónicos que puedan ser evidencia.

Su estructura es:

a) Los principios de la evidencia basada en computadores.
b) Oficiales atendiendo a la escena.
c) Oficiales investigadores.
d) Personal para la recuperación de evidencia basada en computadores.
e) Testigos de consulta externos.
f) Anexos (legislación relevante, glosario y formatos).

**Guía Para El Manejo De Evidencia En IT (Guía Australia) Standards Australia (Estándares de Australia) publico "Guía Para El Manejo De Evidencia En IT" (HB171:2003 Handbook Guidelines for the management of IT evidence) [HBIT03].**

Esta guía no está disponible para su libre distribución, por esto para su investigación se consultaron los artículos "Buenas prácticas en la administración de la evidencia digital" [BueAdm06] y "New Guidelines to Combat ECrime" [NeGu03]. Es una guía creada con el fin de asistir a las organizaciones para combatir el crimen electrónico. Establece puntos de referencia para la preservación y recolección de la evidencia digital. Detalla el ciclo de administración de evidencia de la siguiente forma:

a) Diseño de la evidencia.
b) Producción de la evidencia.
c) Recolección de la evidencia.
d) Análisis de la evidencia.
e) Reporte y presentación.
f) Determinación de la relevancia de la evidencia.

# ANEXO - B

## FORMATO DE INFORME PERICIAL

Las y los peritos presentarán su informe de conformidad con lo establecido en los artículos 19 y 20 del REGLAMENTO DEL SISTEMA PERICIAL INTEGRAL DE LA FUNCION JUDICIAL. Por lo tanto, el presente formato puede ser considerado por los auxiliares de justicia para la presentación de los informes periciales, sin perjuicio a lo establecido en normas legales específicas.

**"INFORME PERICIAL"**

1. **DATOS GENERALES DEL JUICIO, O PROCESO DE INDAGACIÓN PREVIA**

| | |
|---|---|
| **Nombre Judicatura o Fiscalía** | |
| **No. de Proceso** | |
| **Nombre y Apellido de la o el Perito** | |
| **Profesión y Especialidad acreditada** | |
| **No. de Calificación** | |
| **Fecha de caducidad de la acreditación** | |
| **Dirección de Contacto** | |
| **Teléfono fijo de contacto** | |
| **Teléfono celular de contacto** | |
| **Correo electrónico de contacto** | |

1. **PARTE DE ANTECEDENTES**, en donde se debe delimitar claramente el encargo realizado, esto es, se tiene que especificar claramente el tema sobre el que informará en base a lo ordenado por el juez, el fiscal y/o lo solicitado por las partes procesales.

2. **PARTE DE CONSIDERACIONES TÉCNICAS O METODOLOGÍA A APLICARSE**, en donde se debe explicar claramente, cómo aplican sus conocimientos especializados de su profesión, arte u oficio, al caso o encargo materia de la pericia. La o el perito deberá relacionar los contenidos de sus conocimientos especializados con el objeto de la pericia encargada. Analizará si son pertinentes o no la aplicación de sus conocimientos especializados al caso concreto materia de su informe.

3. **PARTE DE CONCLUSIONES,** luego de las consideraciones técnicas, se procederá a emitir la opinión técnica, o conclusión de la aplicación de los conocimientos especializados sobre el caso concreto analizado. Se prohíbe todo tipo de juicios de valor sobre la actuación de las partes en el informe técnico. El informe solamente versará sobre los hechos consultados y ordenados, establecidos en los antecedentes, y nada dirá sobre el accionar de las partes procesales en el caso en particular. Las conclusiones solamente se referirán a los temas materia de la pericia debidamente delimitados y explicados en los antecedentes. Cualquier otro criterio adicional a la delimitación de la pericia no será tomado en cuenta al momento de resolver, y será tomado en consideración para la evaluación de la o el perito.
4. **PARTE DE INCLUSIÓN DE DOCUMENTOS DE RESPALDO, ANEXOS, O EXPLICACIÓN DE CRITERIO TÉCNICO**, deberá sustentar sus conclusiones ya sea con documentos y objetos de respaldo (fotos, copias certificadas de documentos, grabaciones, etc); y/o, con la explicación clara de cuál es el sustento técnico o científico para obtener un resultado o conclusión específica. Se debe exponer claramente las razones especializadas de la o el perito para llegar a la conclusión correspondiente. No se cumplirá con este requisito si no se sustenta la conclusión con documentos, objetos o con la explicación técnica y científica exigida en este numeral. La o el perito deberá razonar y motivar diáfanamente la razón de sus dichos, esto es, justificar desde todo punto de vista las conclusiones que incluya en el informe. En caso de que no fundamente sus conclusiones y esto sea informado por el juez, la jueza, o el/la fiscal, será considerado al momento de la evaluación de la o el perito.

5. **OTROS REQUISITOS,** si la ley procesal correspondiente determina la inclusión de requisitos adicionales a los establecidos por el reglamento, la o el perito debe hacerlo constar necesariamente en su informe pericial de conformidad con dicha exigencia legal.

6. **INFORMACIÓN ADICIONAL,** la o el perito podrá incluir cualquier otro tipo de información adicional a los numerales anteriores, siempre y cuando la misma ayude a clarificar sus explicaciones y/o conclusiones; siempre y cuando esta información se encuentre dentro de los límites del objeto de la pericia.

7. **DECLARACIÓN JURAMENTADA,** la o el perito deberá en la parte final del informe, declarar bajo juramento que su informe es independiente y corresponde a su real convicción profesional, así como también, que toda la información que ha proporcionado es verdadera.

8. **FIRMA Y RÚBRICA,** al final del informe se deberá hacer constar la firma y rúbrica de la o el perito, el número de su cédula de ciudadanía, y el número de su calificación y acreditación pericial."

**Nota: el presente ejemplar es una guía de los ítems que al menos deben considerar los auxiliares de justicia al momento de elaborar sus informes periciales.**

# ANEXO - C

**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.<br>Fases<br>1. Identificación de evidencia. - facilitada por la parte actora.<br>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.<br>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<br>- 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<br>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:<br>- En primer lugar, se procedió a fijar fotográficamente el material recibido para peritación (estuche o sobre contenedor).<br>- Se retiran las seguridades con las que contaba el DVD-R sacándolo del estuche que lo contenía.<br>- Se procedió a verificar visualmente la integridad física del DVD-R, no encontrando alteraciones en su estructura.<br>- 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.<br>- Se procede a realizar la explotación de la cuenta de la red social de Facebook del denunciado Orlin Israel Castro Vásquez.<br>- Se procede a verificar las publicaciones de fecha.<br>- 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.<br>- 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<br>- 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:<br>1. Búsqueda de datos relevantes para el análisis.<br>2. Identificación y categorización de los datos encontrados.<br>3. Comprobar integridad de los datos.<br>4. Identificar importancia de los datos para la investigación y<br>5. Realizar conclusiones sobre los datos obtenidos |
| Herramientas utilizadas en la pericia | - Software para el cálculo del Hash MD5<br>- 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:<br>1. Generación de una imagen forense del CD con número de serie: TBZ705154624E17<br>2. Extracción e identificación de los archivos presentes en la unidad de almacenamiento.<br>3. Creación de imágenes de los archivos de video existentes en la unidad de almacenamiento,<br>4. Transcripción de audio de los archivos de la unidad de almacenamiento.<br>5. Correlacionar imágenes creadas y transcripción realizada.<br>6. Realizar conclusiones sobre los datos obtenidos. |
| Herramientas utilizadas en la pericia | - Encase: software para generar imagen forense del CD<br>- 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:<br>• Identificación: identificar las evidencias |

| | |
|---|---|
| | • Recolección: determinar fuentes de información, adquisición o extracción mediante técnicas y herramientas<br>• Análisis: examinar la información obtenida<br>• Resultados: elaboración y entrega de informe pericial<br>Técnicas aplicadas:<br>• Reconocimiento o footprinting<br>• Procedimiento ELA (análisis de errores de nivel)<br>• Técnica inversa de imágenes |
| Herramientas utilizadas en la pericia | • FotoForensics<br>• Google Images<br>• Herramienta de desarrollo de la página web<br>• 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:<br>• Origen de la publicación<br>• Número de veces que la publicación es compartida.<br>• Número de reacciones emitidas o generadas en la publicación. |
| Metodología aplicada | • Revisión de código fuente HTML.<br>• Se identifica el nombre de usuario con su respectivo ID de la cuenta de Facebook.<br>• Verificar el URL de origen.<br>• 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<br>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<br>2. Generación de Hash del archivo<br>3. Análisis de Meta Data<br>4. Conclusiones<br>5. Inclusión de documentos de respaldo o anexos |
| Herramientas utilizadas en la pericia | • MD5 & SHA Checksum Utility 2.1<br>• 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)<br>• 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<br>- Descripción del objetivo de análisis<br>- Prueba pericial<br>- 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<br>- AccessData FTK Imager 3.1 para<br>- 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:<br>1. Antecedentes<br>2. Planteamiento del problema<br>3. Verificación<br>4. Conclusiones |
| Herramientas utilizadas en la pericia | ADOBE AUDITION CC 2018<br>Se realiza la transcripción de los audios manualmente |

| | |
|---|---|
| Número de juicio | 17308-2011-1444 |
| Tema | Verificar:<br>• 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<br>• Determinar si el sistema indicado, cuenta adicionalmente con el desarrollo informático complementario, especial para la empresa TRAMACOEXPRESS<br>• Las bondades y usos que puede brindar el sistema analizado<br>• 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.<br>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:<br>La evidencia debe ser adquirida del modo menos intrusivo posible.<br>Análisis de metadatos. (propiedades internas de un archivo)<br>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.<br>- Verificar la calidad de audio, de existir ruido ambiental, realizar suavizado del mismo.<br>- Identificar a los locutores que intervienen en la grabación y asignar un código o nombre personalizado.<br>- Transcribir la conversación identificando tiempo, locutor y contenido de la conversación. |
| Herramientas utilizadas en la pericia | - Adobe Audition<br>- 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<br>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<br>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.<br>- Indexación de documentos para elaborar un mapa de archivos.<br>- Materialización de muestras por un total de 5 ejemplares.<br>- Clasificación de documentos.<br>- Anillado de documentos.<br>- 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<br>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<br>2. Detalles técnicos del archivo |
| | 3. Comparativa con respecto al tiempo de la zona analizada. |
| Herramientas utilizadas en la pericia | Google Earth Pro<br>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<br>- 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.<br>- 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<br>- La aplicación en línea SpeechLogger que procesa la información del audio del computador y hace uso del Driver anteriormente manifestado.<br>- 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.<br>- Enlistar los dispositivos entregados. |
| | - Verificar los números de serie de los dispositivos.<br>- Enlistar las audiencias que se grabaron con dichos equipos.<br>- Determinar el funcionamiento de los equipos.<br>- Verificar si el sistema de grabación de audiencias Cicero fue borrado. |
| Metodología aplicada | - Las prácticas técnicas consistieron en:<br>- Comunicación con personal de Unidad Judicial de familia, mujer y adolescencia solicitando permiso y facilidades para efectuar el peritaje informático.<br>- Observación de las instalaciones<br>- Revisión de la documentación<br>- Inspección de los equipos entregados mediante actas entrega recepción<br>- Levantamiento de información<br>- Recolección de evidencia<br>- Documentación fotográfica.<br>- Probar el software para grabación de audiencias.<br>- Verificar estado del Software CICERO |
| Herramientas utilizadas en la pericia | - Software Cicero<br>- 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.<br>- Enlistar los dispositivos entregados.<br>- Verificar los números de serie de los dispositivos.<br>- Enlistar las audiencias que se grabaron con dichos equipos.<br>- Determinar el funcionamiento de los equipos. |
| Metodología aplicada | - Reunión con personal de la Dirección Nacional de TICS<br>- Observación de las instalaciones<br>- Revisión de la documentación<br>- Inspección de los equipos entregados mediante de actas entrega y recepción<br>- Levantamiento de información<br>- Recolección de evidencia<br>- Documentación fotográfica.<br>- 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.<br>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<br>- 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.<br>- Buscar la cuenta @**sa y obtener acceso a los tweets recientes publicados en la misma.<br>- Determinar que el titular de la cuenta @*** de acuerdo con la información mostrada por Twitter.<br>- Se procedió a cargar los tweets publicados por la cuenta @**esa durante el mes de enero del 2014.<br>- 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.<br>- Autenticarse en el sistema y acceder a los registros referentes al ciudadano.<br>- Extraer información correspondiente.<br>- 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.<br>- 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<br>- Verificar bandeja de entrada<br>- Buscar en la bandeja de entrada correo con dominio "arcom.gob.ec"<br>- 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<br>- Acreditar la veracidad de los mismos, origen fechas y desmaterialización completa de los mismos. |
| Metodología aplicada | - Acceder al servidor de correo electrónico<br>- Identificar las cuentas de correo, obrantes<br>- Ordenar los correos electrónicos por la fecha, verificando que el correo más antiguo que consta como recibido en el buzón<br>- Corroborar la veracidad de los mensajes comprobando que fueron enviados atreves del servidor de correo que la empresa Tedasa S.A<br>- 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:<br>- 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<br>- Extraer los correos pertinentes<br>- - 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<br>- Entrevista con el área de nóminas para revisar el funcionamiento del usuario por parte del aplicativo<br>- Explicación del Registro de Entrada y Salida<br>- 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.<br>- Buscar el usuario en el sistema.<br>- 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<br>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.<br>- 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.<br>- 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<br>- 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<br>- Tablero de energía<br>- Generador eléctrico<br>- Equipos de radio frecuencia<br>- Torre Monopolo<br>- 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#<br>Se busca el contacto requerido<br>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.<br>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.<br>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.<br>- Realizar la extracción del código HASH MD5 del archivo.<br>- Se realiza la transcripción de la entrevista.<br>- Se procede a materializar la entrevista. |
| Herramientas utilizadas en la pericia | Programas de ofimática<br>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.<br>- Fijar fotográficamente el CD-R (lado frontal y lado posterior).<br>- Se procedió a verificar visualmente la integridad física del CD-R, no encontrando alteraciones en su estructura.<br>- Se verifica visualmente indicios de escritura en la superficie fotosensible del CD-R no observando rastro alguno.<br>- 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<br>Oracle<br>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.<br>Digital Forensics Framework<br>Para revisión de los videos se utilizó el Reproductor de Windows Media<br>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.<br>- Verificar visualmente la integridad física del CD-R con el programa "Reproductor de Windows Media" para la visualización de videos (Imagen y Sonido)<br>- Verificar la calidad y contenido de la grabación del archivo de video que obra en el CD-R objeto de análisis.<br>- 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<br>- Verificación de contenido<br>- Extracción de información desde la cuenta personal de correo electrónico del señor Marco Tulio Giler Mendoza<br>- 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<br>- Recopilación y extracción de información del perfil de usuario de Carlos Andrés Giler Castillo<br>- Información recopilada del perfil de usuario de Fabian Alvarado<br>- Extracción de Información desde la aplicación WhatsApp configurada con el número 0983392558 instalada en el teléfono HUAWEI Ascend Y530.<br>- 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<br>- Revisar las marcaciones de ingreso y salida en la bitácora del demandante<br>- 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<br>- Buscar y obtener los correos electrónicos del servidor de la organización<br>- Fijación de los correos |

| | |
|---|---|
| | - Extraer y materializar los correos electrónicos y los adjuntos que existen en los correos electrónicos<br>- Extraer y materializar los adjuntos que existen en los correos electrónicos.<br>- Obtener las cabeceras de los correos electrónicos. |
| Herramientas utilizadas en la pericia | Servidor de correo para extracción de información<br>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.<br>- Búsqueda de la noticia con el código señalado.<br>- 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<br>- Recolección de información mediante consultas al sistema.<br>- Determina existencia de evidencia en el sistema<br>- 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<br>- 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.<br>Generar los reportes necesarios para su posterior análisis. |
| Metodología aplicada | - Acceder a las opciones solicitadas junto a la persona que genero los reportes<br>- Analizar el primer reporte que es el comprobante de pago<br>- 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.<br>2. En el caso del sistema DATAACROM, se accedió con el usuario LBERMEO que aún seguía activo |
| Herramientas utilizadas en la pericia | Sistema QUIPUX<br>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.<br>- 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<br>2. Revisar el contenido de la memoria<br>3. Realizar una búsqueda minuciosa de cada carpeta<br>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.<br>- 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<br>- Revisar las características del celular que fue entregado<br>- 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<br>Sistema de Active Directory de Windows Server 2012<br>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.<br>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.<br>- Ingresar al computador con la finalidad de ingresar al software CICERO, y poder verificar las audiencias que se encuentran grabadas.<br>- Revisar el directorio VIDEOCICERO que contiene archivos de audio. |
| Herramientas utilizadas en la pericia | Software CICERO<br>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.<br>- 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<br>- Verificar IMEI<br>- Extracción del grabado<br>- 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.<br>- Determinar calidad de videos<br>- 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<br>- Se transcribió el contenido<br>- 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<br>- Verificar que corresponden en su contenido a los enviados por el compareciente<br>- 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<br>1. Inspección de los trabajos de digitalización e indexación<br>2. Reconocimiento en área de tecnología<br>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<br>- Determinar ubicación del archivo<br>- Extraer los archivos .jpg |

| | |
|---|---|
| Herramientas utilizadas en la pericia | FTK Imager para generar la imagen forense y exportar los archivos de tipo fotográfico<br>HashCalc para generar el código hash de los archivos<br>Para la obtención de los metadatos:<br>- JPGSNOOP<br>- 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:<br>- Recepción del correo.<br>- Asunto, fecha y hora del email.<br>- Autenticidad y a quién pertenece la dirección de email.<br>- Contenido textual del email.<br>- Personas a las que se les envío copia del correo.<br>- Dirección IP del correo.<br>- Dirección desde donde se emitió el correo electrónico. |
| Metodología aplicada | - Se inicia buscando el correo electrónico en el programa Hotmail.<br>- Se realizó el cotejamiento de los distintos buzones con el correo electrónico objeto de la pericia.<br>- Obtención de la cabecera del correo electrónico localizado.<br>- 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<br>ToolBox Google |

| | |
|---|---|
| Número de juicio | 17554-2017-00005 |
| Tema | Desmaterialización del contenido de un CD |
| Metodología aplicada | - Análisis del CD, revisión de meta data<br>- Identificar personas que intervienen en el video<br>- 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.<br>- Validar la información obtenida.<br>- Capturar pantallas con datos que demuestren la información solicitada a CNT.<br>- 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.<br>- 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.<br>- 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.<br>- Se realizó el cotejamiento de los distintos buzones con el correo electrónico objeto de la pericia.<br>- Obtención de la cabecera del correo electrónico localizado en el programa Outlook.<br>- 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<br>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<br>- 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<br>Generador de código Hash no especificado. |

| | |
|---|---|
| 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<br>- Entrevista con la responsable/administradora del sistema biométrico<br>- Análisis del equipo mediante el cual se administra el sistema biométrico<br>- 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<br>- Evidenciar todos los módulos instalados en el Sistema Integrado de Gestión Municipal ERP CABILDO<br>- Comprobar y evidenciar, que se encuentra instalado el motor de la Base de Datos ORACLE<br>- Verificar que existe un crecimiento de la Base de Datos<br>- 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<br>- 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<br><br>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<br><br>Plataforma de Global Inter Gold |

| | |
|---|---|
| Número de juicio | 17371-2016-00673 |
| Tema | Extraer información de correo electrónico |
| Metodología aplicada | - Recopilación de información, claves facilitadas<br>- Verificar información<br>- 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<br>- Verificar existencia del dispositivo<br>- Revisión del funcionamiento del reloj biométrico |

| | |
|---|---|
| | - Ejecución del software de control y del dispositivo<br>- 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<br>- Determinar si la página web, dirección electrónica Milhojas.is/61242-la-ruta-criminal.del-oro-ecuatoriano-html es real e identifica quien más compartieron.<br>- 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<br>- 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"<br>Visual Basic 6.0.<br>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<br>- Buscar correos de interés<br>- 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.<br>Se revisa el procedimiento de ingreso de un nuevo empleado.<br>Se obtiene información del reloj biométrico.<br>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.<br>- 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<br>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<br>- 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:<br>- La existencia y ubicación del reloj biométrico.<br>- Que la memoria o CPU no ha sido manipulada o alterada.<br>- 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. |