PERITO INFORMÁTICO JUDICIAL FORENSE

Juan Pablo Luna Felipez, M.Sc.
jplunaf@gmail.com

Docente Ingeniería Informática
Universidad Nacional "Siglo XX"
Llallagua , Bolivia

Resumen - *Con el crecimiento exponencial del uso de sitios web, redes sociales y otros, también han surgido nuevas formas de delitos que se conocen como delitos informáticos y se hace necesario profesionales entendidos para apoyar en la investigación de los delitos informáticos.*

El anonimato que da la nube, la pantalla y la cantidad de información que circula libremente, es usado por delincuentes que utilizan la tecnología para cometer infracciones y eludir a las autoridades

Por tanto un nuevo grupo de profesionales ha surgido de la mano del auge de las nuevas tecnologías con una gran demanda: el Perito judicial Informático.

Cada día se va requiriendo más la figura del Perito Informático al proceso judicial, ya que sin duda las nuevas tecnológicas dominan cada sector, industrial, profesional, personal y su pericia e investigación en la localización de evidencias electrónicas hace más necesaria su dictamen como valor probatorio de un procedimiento

Muchas son las personas que saben que contar con un Perito Informático Forense puede ser vital para ganar una demanda y evitar una condena

Sin duda, El Perito Judicial Informático, será el profesional más demandado por una sociedad cada vez más tecnológica y la prueba electrónica es reina en la investigación criminal.

En Bolivia falta mucho camino por recorrer tanto en la parte normativa como en la formación y presencia de estos profesionales.

El presente artículo borda los aspectos inherentes a los peritos judiciales informáticos, sus deberes, responsabilidades, conocimientos, forma de actuación, así como la situación en Bolivia.

Palabras clave - *informática forense, perito judicial informático, perito informático forense, forense informático.*

Abstract - *The exponential growth in the use of web, social networks and other sites also they created new forms of crime which are known as computer crime and is knowledgeable professionals necessary to support in investigating computer crimes.*

Anonymity gives the cloud, the screen and the amount of information flowing freely used by criminals who use technology to facilitate the commission of offenses and elude authorities

Therefore a new group of professionals has emerged from the hand of the rise of new technologies with high demand: the Computer Expert witness.

Each day is going to require more than the figure of Perito Computer judicial process, because without doubt the new technological dominate each sector, industrial, professional, personal and expertise and research in locating electronic evidence more necessary its opinion as probative value a procedure

There are many people who know they have a Computer Forensic Expert can be vital to win a lawsuit and avoid a conviction

Undoubtedly, Perito Judicial Computer, is the professional most demanded by an increasingly technological society

and electronic evidence is queen in the criminal investigation.

In Bolivia a long way to go both in normative part in the training and presence of these professionals.

This article overboard aspects inherent to computer forensic experts, duties, responsibilities, knowledge , forms of action as well as the situation in Bolivia

Keywords - *Computer Forensics, Computer expert witness, Computer expert forensic, Forensic computer expert.*

1. INTRODUCCIÓN

Con el crecimiento exponencial del uso de sitios web, redes sociales y otros, también han surgido nuevas formas de delitos que se conocen como delitos informáticos y se hace necesario profesionales entendidos para apoyar en la investigación de los delitos informáticos.

El anonimato que da la nube, la pantalla del ordenador y la cantidad de información que circula libremente es usado por delincuentes que utilizan la tecnología para cometer infracciones y eludir a las autoridades. (1)

Por tanto un nuevo grupo de profesionales ha surgido de la mano del auge de las nuevas tecnologías con una gran demanda: el Perito judicial Informático.

Cada día se va requiriendo más la figura del Perito Informático al proceso judicial, ya que sin duda las nuevas tecnológicas dominan cada sector, industrial, profesional, personal y su pericia e investigación en la localización de evidencias electrónicas hace más necesaria su dictamen como valor probatorio de un procedimiento judicial (1)

Según Daniel Creus. (2) “un ordenador lo cuenta todo. Sólo necesitamos hacer una copia del disco duro y crear una línea de tiempo de su uso para saber quién ha hecho qué en cada momento, incluso si ha habido intentos de borrar las huellas".

La Administración de Justicia, está comprobando lo infalible y rápido que resulta la localización de las evidencias digitales, que sirven para el esclarecimiento de los caso judicial (1)

Muchas son las personas que saben que contar con un Perito Informático Forense puede ser vital para ganar una demanda y evitar una condena (3)

Sin duda, El Perito Judicial Informático, será el profesional más demandado por una sociedad cada vez más tecnológica y la prueba electrónica es reina en la investigación criminal actual (1)

En Bolivia falta mucho camino por recorrer tanto en la parte normativa como en la formación y presencia de estos profesionales.

2. INFORMÁTICA FORENSE

Según (2) el cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examinación forense digital es “la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Recoge pruebas con extremo cuidado, respetando la cadena de custodia de dichas evidencias”.

Siendo que es una de las áreas que más viene creciendo debido a los delitos informáticos que se dan como indica (4) “la informática forense es una de las disciplinas de la seguridad informática más en auge, más si cabe por el incremento de los delitos informáticos y el cibercrimen”.

También se debe resaltar que esta disciplina es más complicada, porque, en muchos casos, la informática forense se sale de lo puramente técnico y entra de lleno en temas legales, procedimentales y hasta de pura investigación criminal (4)

3. PERITO INFORMATICO FORENSE

Según (1) el perito Judicial Informático o Perito Informático Forense “es un profesional dotado de los conocimientos especializados en las nuevas tecnológicas, a través de su capacitación y experiencia, que suministra información u opinión fundada a profesionales, empresas y a los tribunales de justicia sobre los puntos litigiosos que son materia de su dictamen”

Por tanto es el encargado de analizar los elementos tecnológicos, y buscar aquellos datos que puedan constituir la evidencia digital que permitirá el esclarecimiento del litigio al que ha sido asignado en un proceso legal, aportando seguridad, conocimientos y demostrando aquellos aspectos tecnológicos que no están obligados a conocer profesionales del derecho o tribunales. (5)

3.1 NOMBRAMIENTO

Existen dos tipos de peritos informáticos forenses: los nombrados judicialmente y los propuestos por una o ambas partes del litigio, aceptados por el juez o el fiscal, y ambos ejercen la misma influencia en el juicio (6)

Cuando un Perito Informático es nombrado por un Juez, Magistrado o Administración, automáticamente se convierte en auxiliar de la justicia y debe realizar la función pública de acuerdo con el cargo conferido y se rigen por las leyes y reglamentos especiales (1)

3.2 OBJETIVOS

El objetivo principal del Perito Informático forense es el de "recuperar los registros y mensajes de datos existentes dentro de un equipo informático, de tal manera que toda esa información digital, pueda ser usada como prueba ante un tribunal" (1)

También busca otros objetivos secundarios entre los que se menciona (2):

- Describir de manera clara el incidente de seguridad
- Describir posibles consecuencias del mismo
- Identificar al autor del incidente de seguridad
- Valorar la defensa jurídica / actuación de las Fuerzas del Estado
- Post-mortem análisis forense como medida de mejora en la política de seguridad actual.

3.3 REQUISITOS

Para ejercer como Perito informático forense primordialmente es indispensable una titulación oficial. (5)

Sin embargo también se hace necesario cursos de especialización en el área de Informática forense.

3.4 CUALIDADES

El Perito Judicial Informático debe tener ciertas cualidades adecuadas para su correcta función, según (1) entre estas se tiene las siguientes:

(a) Integridad intachable para determinar neutralmente los hechos sin ninguna preferencia o afición por ninguna de las partes.
(b) Poseer conocimientos legales en derecho procesal civil, penal, administrativo y laboral que le permitan desarrollar su tarea sin que la misma sea descalificada o impugnada durante su presentación judicial.
(c) Experto en conocimientos forenses, siendo de vital importancia que esté familiarizado con las evidencias electrónicas.
(d) Formación pragmática y académica la adquisición de habilidad técnica y científica usando un lenguaje científico, no cientificista, que permita al profano en esta ciencia comprender el mismo (1)

3.5 DEBERES

El perito informático forense tiene los siguientes deberes (3):

- Aceptar el cargo que le es asignado.
- Colaborar con el resto de los peritos o consultores técnicos
- Declarar ante el juez en el caso de que este lo requiera.
- Fundamentar sus conclusiones técnicas, expresando claramente los elementos analizados y las técnicas utilizadas para llegar a las mismas.
- Respetar el código de ética que le impone su profesión.

3.6 ÁREAS DE ACTUACIÓN

Las áreas de actuación del perito informático forense de acuerdo con (3) y (1) son los siguientes:

- Propiedad industrial: espionaje y/o revelación de secretos.
- Acceso o copia de ficheros de la empresa, planos, fórmulas, costes.
- Uso de información: Competencia desleal de un empleado.
- Vulneración de la intimidad. Lectura de correo electrónico.
- Despido por causas tecnológicas.
- Valoraciones de bienes informáticos.
- Interceptación de telecomunicaciones.
- Protección de datos personales y datos reservados de personas jurídicas.
- Apoderamiento y difusión de datos reservados.
- Manipulación de datos o programas.
- Valoraciones de bienes informáticos.
- Instalaciones y desarrollos llave en mano.
- Vulneración de la buena fe contractual.
- Publicidad engañosa, competencia desleal. Delitos económicos, monetarios y societarios.
- Delitos contra el mercado o contra los consumidores.
- Delitos contra la propiedad intelectual.

- Uso de software sin licencia. Piratería.
- Copia y distribución no autorizada de programas de ordenador.
- Daños mediante la destrucción o alteración de datos.
- Sabotaje. Estafa, fraudes, conspiración para alterar el precio de las cosas.
- Pornografía infantil: acceso o posesión, divulgación, edición.
- Uso indebido de equipos informáticos: daños o uso abusivo

3.7 CONOCIMIENTOS

De acuerdo con (4) los dominios principales del conocimiento que debe poseer un perito informático forense son:

(a) Metodologías de análisis forense: Para identificar, adquirir, conservar y recuperar evidencias digitales y presentar hechos objetivos a partir de su análisis, siguiendo las metodologías de forma estricta.

(b) Procedimientos forenses y legales: La informática forense está en muchos casos estrictamente regulada, y hay que conocer los procedimientos establecidos

(c) Respuesta ante incidentes: La informática forense en muchos casos se integra dentro de la respuesta ante incidentes, por lo que es necesario el conocer las bases de la misma

(d) Manejo de laboratorios forenses: Es necesario disponer de las herramientas necesarias para realizar todos los procedimientos de respuesta y su posterior análisis. Máquinas virtuales, servidores, almacenamiento, hardware de adquisición de datos, etc…

(e) Gestión de evidencias digitales: Para la correcta identificación, adquisición y conservación de todos los soportes que puedan contener evidencias digitales

(f) Sistemas de ficheros: Cada sistema de ficheros (FAT, NTFS, ext4) tiene su estructura y sus peculiaridades. El conocerlas es fundamental para poder recuperar información y poder extraer todos los datos

(g) Recuperación de datos: La primera fase de un análisis forense es la recuperación de datos de todos los soportes adquiridos. Desde los ficheros en la papelera hasta aquellos borrados (pero en muchos casos recuperables), y llegando hasta el *file carving* (recuperación parcial de ficheros)

(h) Sistemas operativos: Es fundamental conocer lo más a fondo posible el funcionamiento de los sistemas operativos más comunes (Windows, Linux y Mac) para sacar el máximo juego a la información. Redes: Hoy en día casi todos los crímenes tienen una red como medio. Ya sea una ADSL, WLAN, 3G o Bluetooth, hay que saber los entresijos de cada una de ellas , también hay que tener en cuenta el análisis de tráfico, vital para detectar una botnet u obtener más pruebas de un delito en vivo.

(i) Móviles y tablets: La permeabilidad de móviles y tablets en la sociedad actual es innegable. Y son verdaderos tesoros para un analista forense, desde los contactos de la SIM hasta los mensajes de Whatsapp o la propia localización de los terminales (que está en poder de las operadoras de telecomunicaciones).

(j) Análisis de memoria RAM: Los datos volátiles ofrecen muchísima información, desde malware que reside únicamente en memoria hasta las contraseñas de sitios web que están contenidas en su interior

(k) Análisis de *logs* y correlación de eventos: Toda acción deja una huella (principio de Locard, una de las bases de la ciencia forense) y los *logs* son los mejores amigos.

(l) Generación de líneas temporales: Una técnica de análisis forense muy potente es realizar una línea temporal basándose en los tiempos MAC (Modificado, Accedido, Cambiado) de cada fichero.

(m) Imagen, audio y vídeo: El análisis de contenido multimedia, sobre todo en términos de garantizar su autenticidad e integridad, es fundamental.

(n) Navegadores: Lo primero que suelen hacer los usuarios a día de hoy cuando encienden su ordenador es arrancar un navegador. Desde el historial de páginas visitadas a las *cookies* o los sitios en los que se ha guardado la contraseña, los navegadores son una verdadera mina de oro para los analistas forenses.

(o) Clientes de correo: Ya sean clientes físicos o

basados en web como Gmail, los correos electrónicos (y sobre todo el análisis de sus cabeceras) son una fuente primordial de información a la hora de investigar un posible delito.

(p) Software P2P: Emule, Ares, uTorrent… todos ellos usados para la descarga de contenidos más o menos legales, y sobre todo muy usado en temas de pornografía infantil. El conocer cómo funcionan estos programas y cómo comparten ficheros es fundamental.

(q) Redes sociales: Facebook y Twitter saben más que nuestros ancestros. El saber qué tipos de información y cómo se configura la privacidad y seguridad de las redes sociales más conocidas nos puede dar muchísima

(r) Detección y análisis de malware: El *malware* es cada vez más sofisticado y dirigido a cometer delitos. El conocer cómo infectan y atacan los últimos troyanos (y el saber detectar la presencia de uno en un sistema) es fundamental.

(s) Cibercrimen: El 99% del *malware* está dirigido a la obtención de dinero, y hay un verdadero ecosistema detrás de cada troyano bancario. Muleros, *carders, bot herders* …

(t) *Cloud Computing:* La nube está cambiando en muchos casos la forma de interactuar con la tecnología. El conocer cómo funcionan muchos programas que trabajan en la nube (como Dropbox o Flickr para documentos y fotos, o si nos vamos a servidores completos como los que provee Amazon Web Services) es fundamental.

(u) Metadatos: Casi todos los documentos que generamos tienen metadatos que dan muchísima información. Un documento Word, un .pdf, o una foto tomada por una cámara digital o un móvil pueden tener la clave de una investigación.

(v) Bases de datos: El análisis forense de bases de datos es crítico sobre todo en casos de fraude. El saber qué usuario accedió a qué datos en qué momento, o si los controles de acceso pertinentes estaban bien configurados nos puede ayudar a identificar a un posible culpable.

(w) Legislación: La informática forense está fuertemente relacionada con la comisión de delitos, por lo que es necesario conocer la legislación vigente al respecto.

(x) Técnicas de investigación: Aunque en esta parte entre en juego la intuición y el instinto de cada uno, hay muchas técnicas que pueden ser aprendidas.

(y) Redacción de informes forenses: Todo el análisis realizado debe de ser ordenado, recopilado y presentado en forma de hechos demostrables. No existe lugar para las suposiciones u opiniones personales, tan solo para los hechos.

(z) Defensa de informes forenses: En muchos casos es muy posible debamos testificar como peritos, defendiendo nuestro informe en un juicio, contestando tanto a las preguntas del jurado como a las del abogado de la otra parte. El saber exponer conceptos técnicos de forma clara, y el saber contestar las preguntas son dos aptitudes que hay que dominar.

(aa) Ética: En un juicio, ya sea civil o penal, una o varias personas se están jugando mucho dinero, o incluso ir a la cárcel. La objetividad y el comportamiento estrictamente ceñido a la verdad y a los hechos probados son absolutamente necesarias para un analista forense.

3.8 FUNCIONES

Las principales funciones de un Perito informático forense son las de: asesorar, emitir informes judiciales o extrajudiciales, siendo su papel el de auxiliar de Magistrados, Jueces, Abogados, Tribunales. (5)

Todo ello a partir de sus conocimientos científicos y técnicos siendo su papel el de auxiliar de Magistrados, Jueces, Abogados, Tribunales y a cuantas personas lo necesiten a través de sus conocimientos según lo dispuesto en la leyes.

En su carácter de auxiliar de la justicia tiene como tarea primordial la de asesorar al juez respecto a temas relacionados con la informática (3)

3.9 TAREAS

Las tareas a desarrollar por el perito informático forense no son distintas de la de otros peritos judiciales.

Por lo tanto deberá recopilar la información que es puesta a su disposición, analizar la misma en busca de los datos que el juez le ha requerido y emitir un informe o dictamen en donde vuelque las conclusiones de la investigación realizada (1)

En ese afán el perito informático forense tecnológico hará un estudio de cómo ocurre un incidente informático, quién lo ejecuta, por qué y con qué objetivo, este análisis siempre basado en la recolección de las evidencias digitales. (1)

La recolección de evidencias digitales (o evidencias electrónicas) se constituye en una de las facetas útiles dentro del éxito de en una investigación criminal, aspecto que demanda de los Peritos Informáticos encargados de la recolección preservación, análisis y presentación de las evidencias digitales una eficaz labor que garantice la autenticidad e integridad de dichas evidencias, a fin de ser utilizadas posteriormente ante el Tribunal (1).

Mediante su juicio científico-técnico, debe dictaminar con veracidad e imparcialidad, opinando y emitiendo conclusiones sobre puntos concretos relacionados con hechos o circunstancias, sus causas o efectos, para cuya apreciación son indispensables conocimientos especializados. (1)

El dictamen final del Perito Judicial Informático, es una declaración de ciencia que debe sustentarse en reglas probadas, lógicas y verificadas que prevalecen en su cultura científico-técnica, y ha de valerse de los procedimientos técnicos forenses en medios electrónicos que fortalecen y desarrollan una línea de investigación forense en informática (1)

4. INFORMÁTICA FORENSE Y PERITOS INFORMÁTICOS FORENSES EN BOLIVIA

4.1 NORMATIVA BOLIVIANA

Si bien Bolivia cuenta con normativas para las diversas áreas, en relación al tema netamente informático aún falta mucho camino por recorrer a diferencia de otros países como España.

El capítulo XI del Código Penal Boliviano dictamina la reclusión de uno a cinco años y una multa de 60 a 200 días para la persona que cometa el delito de manipulación informática. Mientras que el artículo 363 ter sanciona con prestación de trabajo de hasta un año o una multa de hasta 200 días al involucrado en la alteración, acceso y uso indebido de datos informáticos.

Textualmente ambos artículos indican:

Articulo 363.-bis (MANIPULACIÓN INFORMÁTICA).El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

Articulo 363.-ter (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS). El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días."

4.2 ESTADÍSTICAS Y DATOS

En Bolivia se cuenta con el sistema IANUS, que es un sistema informático que realiza un seguimiento computarizado de los procesos que se ventilan a nivel nacional, y que sirve a los jueces de instrumento para organizar su trabajo y controlar los plazos, con el objetivo de evitar la retardación de justicia (7).

Según datos del sistema IANUS, De 2002 a 2011, los juicios por delitos informáticos crecieron en 890%, de ocho a 79, de los cuales 62 están referidos a manipulación informática y 17, a la alteración, acceso y uso indebido de datos informáticos. Aparte, en esa década, los juzgados paceños recibieron 228 causas referidas al primer delito y 15 del segundo.

Según la Fuerza Especial de Lucha Contra el Crimen (FELCC) y el Consejo de la Magistratura de La Paz, el 2012 recibió 574 denuncias referidas a manipulación informática en ocho departamentos, menos en Oruro. Doce más (casi 2%) que las 562 que llegaron a sus oficinas en 2010 (7)

El incremento demuestra que, cada día, los delincuentes se apoyan más en las herramientas de la tecnología para realizar actos reñidos con la ley

4.3 ¿QUIENES INVESTIGAN LOS DELITOS INFORMÁTICOS EN BOLIVIA?

Según el coronel Jorge Toro La Policía y el Ministerio Público no están debidamente actualizados en el tema y no cuentan con los medios suficientes para combatir los delitos informáticos (7).

En Bolivia existe el Instituto de Investigaciones Forenses de la Fiscalía que cuenta con equipos para la implementación de informática forense.

Su labor empezó hace más de una década, pero ante la saturación de trabajo en esta entidad, ocho expertos en el rubro se instalaron en el Instituto de Investigaciones Técnico Científicas de la Universidad Policial, que se organizó sobre la base del ex laboratorio de la Policía Técnica Científica, en el barrio de Següencoma, de la zona Sur de la ciudad de La Paz.

Este centro indaga hechos delictivos mediante el estudio de las huellas dejadas en la escena del crimen, la balística, la química legal, la toxicología, la accidentología y otro tipo de pericias, sin embargo su campo de acción se ha extendido a los delitos informáticos, aparte de pesquisas forenses y de genética aplicativa, según el jefe de esta dependencia, el capitán William Llanos, quien es titulado en Ingeniería de Sistemas (7).

En cuanto a los delitos informáticos, analizan medios electrónicos y ópticos para el almacenamiento de información, sean discos duros de computadoras, CD, DVD, celulares; busca portales de pornografía infantil y realiza patrullajes cibernéticos. “Rastreamos páginas de Facebook o sospechosas que intentan reclutar potenciales víctimas para la prostitución. Así dimos con una página en la urbe de Cochabamba” (7).

Estos especialistas tratan de involucrarse con el mundo de las redes dudosas del ciberespacio, hacer amistad y socializar con quienes las operan, para atraparlos, posteriormente, con ayuda de los agentes de la FELCC. “Primeramente creamos un perfil que sigue la corriente al delincuente, llegamos a ser parte de sus contactos de confianza y, luego, empezamos a hacer un operativo más complejo que pasa de lo cibernético a lo físico”, que termina en la detención. Y operan de similar modo cuando van tras las pistas de ciberacosadores o chantajistas informáticos. (7).

Generalmente les llega ordenadores que fueron usados para cometer un delito; su dictamen es considerado como parte del cúmulo de pruebas en los juicios. Para los análisis, añade Llanos, precisan conocer la parte tecnológica y su terminología, y también la parte legal. No obstante, a veces, las normas limitan su accionar. Por ejemplo, la Ley de Telecomunicaciones reconoce desde este año la inviolabilidad de los documentos o archivos particulares que están en un ordenador, lo cual está avalado por la Constitución Política, comenta el investigador. (7).

En el ámbito privado, sobresale la empresa Yanapti, inmersa en la averiguación de delitos informáticos, con un laboratorio forense que se halla provisto con equipos y programas especializados que no contaminan la evidencia digital, y que en la mayoría de los casos accede a la información que los criminales depositaron e intentan borrar de sus computadoras.

Según Claudia Araujo, abogada y experta en seguridad informática de YanapTI en los archivos de casos que residen en su firma, hay “delitos informáticos cometidos pero que no son descubiertos, otros que se descubren pero no son denunciados y otros que fueron denunciados pero nunca llegaron a una sentencia”. Esto último debido a que en el proceso penal se llega a una transacción entre partes, lo que conlleva, generalmente, el resarcimiento del daño a la víctima, tras lo cual ésta desiste de la demanda y cierra y archiva su expediente (7).

4.4 NECESIDAD DE ACTUALIZACIÓN DEL CÓDIGO DE PROCEDIMIENTO PENAL

Es indudable la necesidad de incorporar los temas de los delitos informáticos y la ciencia forense en la legislación Boliviana.

Milton Mendoza, exfiscal y magistrado suplente del Tribunal Constitucional, espera que con el nuevo Código Procesal Constitucional, se abra el principio de “libertad probatoria” para que los testigos presenten soportes informáticos como pruebas, los cuales deben tener autenticidad, precisión y suficiencia para su validez jurídica (7).

12. CONCLUSIONES

Así como debido al crecimiento exponencial del uso de sitios web, redes sociales y otros, han surgido y expandido los delitos informáticos también ha surgido un grupo de nuevos profesionales denominados Peritos judiciales Informáticos.

El Perito Judicial Informático será el profesional más demandado por una sociedad cada vez más tecnológica

Su deber es recopilar la información que es puesta a su disposición, analizar la misma en busca de los datos que el juez le ha requerido y emitir un informe o dictamen en donde vuelque las conclusiones de la investigación realizada

Son nombrados judicialmente y propuestos por una o ambas partes del litigio y para ejercer primordialmente es indispensable una titulación oficial y cursos de especialización en el área de Informática forense.

Las tareas a desarrollar por el perito informático forense no son distintas de la de otros peritos judiciales.

Si bien Bolivia cuenta con normativas para las diversas áreas, en relación al tema netamente informático aún falta mucho camino por recorrer a diferencia de otros países como España.

En Bolivia se tiene presencia del Instituto de Investigaciones Forenses y también existen iniciativas privadas como Yanapti, sin embargo falta mucho camino por recorrer en la formación y presencia de profesionales peritos informáticos forenses.

13. BIBLIOGRAFÍA

1. Elderecho.com. La figura del Perito Judicial Informático. [En línea] Elderecho.com, 26 de 03 de 2012. [Citado el: 27 de 06 de 2016.] http://www.elderecho.com/civil/figura-Perito-Judicial-Informatico_11_385930001.html.

2. GITS. Analisis Forense, Peritos y Detectives Informáticos. [En línea] Gits. [Citado el: 29 de 06 de 2016.] http://www.gitsinformatica.com/forense.html.

3. Informaticos, Asociacion Nacional de Tasadores y Peritos Judiciales. El Perito Judicial Informatico. [En línea] antpji. [Citado el: 29 de 06 de 2016.] http://www.antpji.com/elperitoinformatico.pdf.

4. Incibe. ¿Quieres trabajar en informática forense?. Estos son los principales dominios de conocimiento. [En línea] Incibe.es, 11 de 07 de 2013. [Citado el: 28 de 06 de 2016.] https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/dominios_de_conocimiento_informatica_forense.

5. Security, Forensic &. El Perito Informático Forense Judicial . [En línea] Forensic & Security, 01 de 06 de 2014. [Citado el: 30 de 06 de 2016.] http://forensic-security.com/perito-informatico-forense-judicial/.

6. Wikipedia. Perito judicial. [En línea] Wikipedia. [Citado el: 26 de 06 de 2016.] https://es.wikipedia.org/wiki/Perito_judicial.

7. Razon, La. En La Paz, los juicios por delitos informáticos crecieron 890%. [En línea] La Razon, 07 de 05 de 2012. [Citado el: 1 de 07 de 2016.] **http://www.la-razon.com/index.php?_url=/suplementos/informe/Paz-juicios-delitos-informaticos-crecieron_0_1609639058.html**