EL PERITO INFORMÁTICO EN UN PROCESO LEGAL

Autor: M.Sc. Ing. Elizabeth Mejía García

Email: elymej15@gmail.com

Carrera: Ingeniería Informática

Área Tecnología

Universidad Nacional "Siglo XX"

Llallagua – Potosí – Bolivia

RESUMEN

En la era digital en la que vivimos, los delitos informáticos se han convertido en una preocupación cada vez mayor para individuos, empresas y gobiernos. Estos delitos, que van desde el robo de información confidencial hasta el fraude en línea, pueden tener un impacto devastador en las víctimas y en la sociedad en su conjunto. Es por eso que la informática forense como parte de las ciencias forenses y los expertos en análisis de evidencia digital juegan un papel crucial en la lucha contra los delitos informáticos. El perito informático tiene un rol fundamental en un proceso legal, destacando la importancia de su trabajo en la recopilación, análisis y presentación de evidencia digital para la resolución de casos que involucran evidencia digital. Cabe aclarar que un ingeniero informático o ingeniero de sistemas por naturaleza no es un perito informático, éste debe tener conocimientos básicos del Derecho, conocer protocolos de actuación frente a delitos informáticos, capacidad en el manejo de técnicas y herramientas de análisis forense digital.

Palabras clave: *evidencia digital, delitos informáticos, informática forense, perito informático*

INTRODUCCIÓN

En la actualidad la justicia está auxiliada por las ciencias forenses que han evolucionado en estos últimos tiempos, en particular la informática forense que aporta evidencias digitales para descubrir, explicar y probar delitos cometidos por cibercriminales. Es innegable que computadoras, teléfonos inteligentes, tabletas con acceso a diferentes aplicaciones de la red internet se han convertido en una parte fundamental de nuestras

vidas, sin embargo, también los cibercriminales están presentes en medios informáticos y ha ido creciendo a medida que las nuevas tecnologías han ido penetrando en la sociedad,

La informática forense es la ciencia que trata la evidencia digital, como ciencia joven, pertenece a las ciencias forenses como medicina forense, balística forense, toxicología forense, etc., tiene fines legales, auxilia a la justicia moderna y se relaciona mucho con la criminalística porque utiliza técnicas como señalética, fotografía, planimetría, rastreo, colecta, protección de la escena del hecho y otras que se adecuan a una investigación criminal de tipo tecnológico, estas pueden ser: estafas electrónicas, acceso y uso indebido de información, falsificaciones informáticas, clonación de tarjetas, pornografía infantil, suplantación de identidad, phising, ingeniería social, cyberbullying, etc., muchos de estos no están tipificados en el código penal.

Para afrontar este tipo de delitos el aparato judicial en nuestro contexto es el principal actor para establecer puntos periciales y ordenar la investigación del hecho delictivo que exige un procedimiento ordenado con la participación de un equipo de especialistas en el área ya que una falla humana puede provocar contaminación o pérdida de evidencias sino se sigue un procedimiento adecuado en la investigación forense, por otro lado juega un papel importante el conocimiento legal, metodológico y técnico del perito que hoy por hoy no está reconocido como perito informático.

METODOLOGÍA

La informática forense es la ciencia que trata la evidencia digital, como ciencia joven, pertenece a las ciencias forenses como medicina forense, balística forense, toxicología forense, etc., tiene fines legales, auxilia a la justicia moderna y se relaciona mucho con la criminalística porque utiliza técnicas como señalética, fotografía, planimetría, rastreo, colecta, protección de la escena del hecho y otras que se adecuan a una investigación criminal de tipo tecnológico. Ante un hecho delictivo el perito informático participa desde el inicio de la investigación hasta la lectura del dictamen en el término del proceso legal, su labor debe centrarse en demostrar la existencia del delito informático y los mecanismos utilizados, teniendo cuidado de enfocarse en los puntos periciales establecidos por la autoridad judicial.

El perito informático como parte del equipo multidisciplinario que acude a la escena del hecho debe estar dotado de herramientas hardware y software forenses que requiere la metodología de la informática forense, el perito informático debe tener la capacidad, habilidad quien con un criterio profesional obtendrá un panorama

general de la escena del crimen, observará e interpretará la situación y el estado de los equipos y dispositivos informáticos del lugar, es el especialista que posteriormente desarrollará el análisis forense de las evidencias y elaborará el dictamen para su presentación en el juicio oral.

De acuerdo a la metodología de la informática forense, en la fase de identificación el perito informático debe tener la capacidad de identificar y evitar que unidades de procesamiento sigan con el flujo de información, considerar unidades de procesamiento, unidades de almacenamiento y unidades de transferencia de información como fuentes de evidencia digital.

En la fase de recolección el perito informático debe tener la capacidad de buscar fuentes de evidencia, debe considerar el Principio de Locard como en cualquier investigación criminalística por lo que las acciones que realice el perito informático deben ser cautelosas para mantener la autenticidad e integridad de las evidencias.

En la fase de preservación debe considerar dos aspectos importantes la preservación física y lógica de los indicios considerando su fragilidad y volatilidad:

En la fase de análisis que se lleva a cabo en el laboratorio de informática forense, antes de proceder con su trabajo pericial se propone que el perito tome en cuenta la estrategia mostrada en la figura 1.

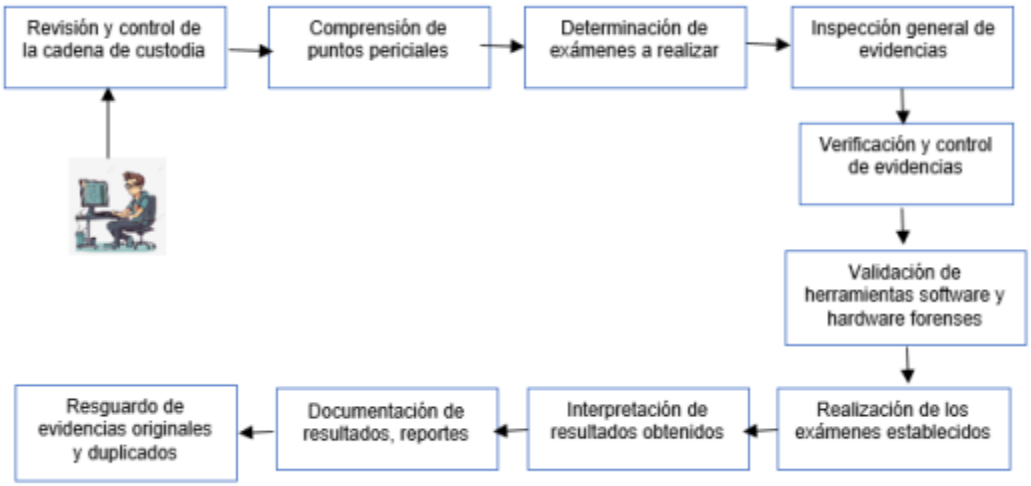

Figura 1: Estrategia del perito informático en el análisis de evidencia digital

Fuente: Elaboración propia

En la fase de presentación el perito informático elabora un informe pericial que incluye todo el procedimiento realizado y los medios que se han utilizado en las diferentes fases de la investigación forense. El informe debe ser redactado de forma clara, evitar en lo posible el uso de términos técnicos ya que normalmente estos

informes serán presentados ante un tribunal penal, donde estarán presentes testigos, abogados, querellantes y que en la actualidad desconocen acerca del funcionamiento profundo de computadoras.

RESULTADOS

Es importante recalcar que la informática forense se aplica cuando ocurre un incidente que involucra evidencia digital y que debe ser tratado por especialistas o peritos informáticos, por lo que el peritaje informático forense se perfila como una de las especialidades que va ir creciendo en el ámbito empresarial como judicial. El perito informático es el especialista en informática forense y debe conocer aspectos legales y de investigación criminalística para precautelar fuentes de evidencia digital y actuar en el marco de la legislación vigente en coordinación con el equipo multidisciplinario que acude a la escena de los hechos.

CONCLUSIONES

Es necesario recalcar la necesidad de relacionar la informática forense con la disciplina jurídica para considerar normas y leyes que regulen las acciones delictivas surgidas en torno a la informática y sus aplicaciones.la criminalística que engloba a las ciencias forenses no puede quedar al margen de delitos que involucra el uso de la tecnología como factor cambiante y dinámico en la sociedad actual, es sabido que la delincuencia está por delante de la policía y los ciberdelincuentes utilizan la tecnología para hacer daño a la sociedad para beneficio personal, razón por la que la criminalística debe estar en constante actualización. Asi mismo el experto en informática forense debe actualizarse y capacitarse continuamente en el uso de herramientas hardware y software forenses, comprender las tendencias en ciberseguridad y delitos informáticos, esto les permitirá mantenerse al día con los métodos cambiantes utilizados por los cibercriminales y proporcionar investigaciones sólidas y concluyentes en un entorno en constante evolución.

> ***“Las contraseñas son como la ropa interior: no dejes que otros las vean, cámbialas con frecuencia y no las compartas con desconocidos” Chris Pirillo***

SOBRE EL AUTOR

Master en Ciencias de la Computación con Mención Seguridad Informática y Software Libre, Master en Educación Superior, Diplomado en Formación Basada en Competencias, Diplomado en Educación Superior, Ingeniero de Sistemas, docente de posgrado en la Universidad Técnica de Oruro, Universidad Pedagógica Sucre, docente titular en la carrera Ingeniería Informática de la Universidad Nacional "Siglo XX", Miembro fundador de la SOCID.

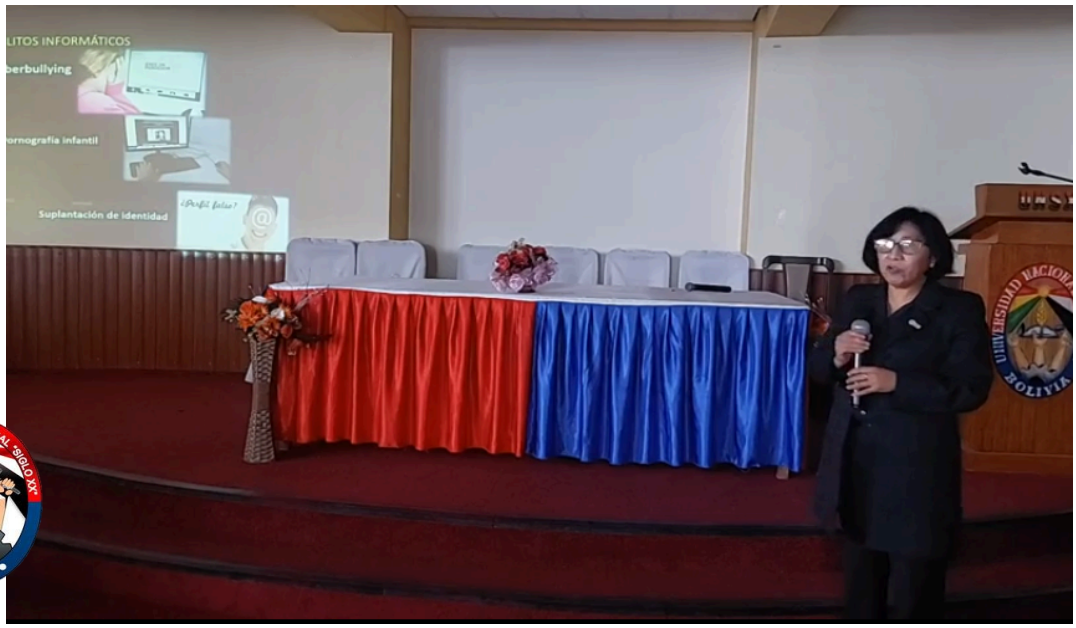

Fig 5. Fotografía de presentación de la ponencia