MODELO DE INFORMÁTICA FORENSE BASADO EN CRIMINALÍSTICA

FORENSIC COMPUTING MODEL BASED ON CRIMINALISTICS

Elizabeth Mejía García
elymej15@gmail.com
Ingeniería Informática
Universidad Nacional "Siglo XX"
Llallagua - Bolivia

Álvaro Rodrigo Calle Maydana
rodrigo.calle.maydana@gmail.com
Perito Informático Forense
Tarija - Bolivia

Resumen- *El presente artículo propone un modelo de actuación para informática forense con base en criminalística, esquema que utiliza la Policía Boliviana frente a un delito tradicional, ya que actualmente en la práctica procesal en Bolivia se observa deficiencias cuando se enfrentan a hechos que involucran evidencia digital. El modelo que se propone se adecua a la metodología de la informática forense desde la identificación de la escena del hecho considerando una protección física y virtual, posteriormente se establecen directrices para identificar indicios tomando en cuenta la cadena de custodia, señaléticas, rastreo, colecta y adquisición de evidencias, preservando la integridad de éstas para evitar contaminaciones y ser analizados por un perito informático con conocimientos técnicos científicos y legales para finalmente redactar el informe pericial y presentar a instancias legales para su defensa.*

Palabras Clave: *Criminalística, Delito informático, Informática forense, Modelo, Procedimiento, Protocolos.*

Abstract- *This article proposes an action model for computer forensics based on criminalistics, a scheme used by the Bolivian Police in the face of a traditional crime, since currently in procedural practice in Bolivia deficiencies are observed when faced with events that involve digital evidence. The proposed model is adapted to the forensic computer methodology from the identification of the scene of the incident considering physical and virtual protection, subsequently guidelines are established to identify clues taking into account the chain of custody, signage, tracking, collection and acquisition of evidence, preserving its integrity to avoid contamination and being analyzed by a computer expert with scientific and legal technical knowledge to finally write the expert report and present it to legal bodies for defense.*

Keywords: *Criminalistics, Computer crime, Computer forensics, Model, procedure, Protocols.*

1. INTRODUCCIÓN

La sociedad actual está viviendo la era Digital, las empresas, instituciones tienen como recurso valioso la información que con el adelanto de la tecnología se ve afectada por ataques informáticos y hechos delictivos en donde se ve involucrado Dispositivos Digitales , este recurso intangible pero valioso está almacenado en ordenadores, teléfonos inteligentes, tabletas y otros con acceso a la red internet y a diferentes aplicaciones que hoy por hoy se han convertido en una parte fundamental de nuestras vidas, sin embargo los cibercriminales están presentes en medios informáticos y también ha ido creciendo a medida que las nuevas tecnologías han ido penetrando en la sociedad, por lo que el peritaje informático forense se perfila como una de las especialidades que va ir creciendo en el ámbito empresarial, policial como judicial. Es así que 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 o delincuentes.

Es indudable que, a comparación de las computadoras tradicionales, los dispositivos móviles se han convertido en una herramienta imprescindible, se usan a nivel personal y profesional para una comunicación diaria, estos dispositivos contienen información como contraseñas, cuentas de correos electrónicos, mensajes de texto, fotos, vídeos, conversaciones privadas, contactos, etc. Por lo que este tiende a ser atacado por cibercriminales, usado por delincuentes o ser medio de prueba dentro de un delito tradicional.

Para afrontar delitos informáticos, el aparato judicial es el principal actor que establece puntos periciales, quienes participan en la investigación forense y deben seguir un protocolo de actuación de informática forense, conocer aspectos legales, metodológicos y técnicos científicos para evitar contaminar o perder evidencias que pueden disminuir el valor probatorio ante la justicia.

Con los antecedentes expuestos anteriormente se puede mencionar que es evidente que en nuestro país los abogados, fiscales, jueces y policías carecen de conocimientos para enfrentar un nuevo reto que es la investigación de un delito informático, por lo que se identifica el problema: ¿Cuál es el protocolo que se debe seguir frente a un caso que involucra evidencia digital?

Para dar respuesta a la pregunta de investigación, se plantea diseñar un modelo de informática forense basado en criminalística a fin de mejorar la eficiencia y efectividad de la respuesta ante casos que involucran evidencia digital, asegurando la integridad de las mismas.

El diseño del modelo conceptual para informática forense se constituye en una propuesta de actuación frente a delitos informáticos y casos donde se ven involucrados dispositivos digitales, ya que actualmente el personal a menudo no está capacitado en esta área, lo que puede resultar en la pérdida de evidencias importantes. El modelo consta de fases relacionadas con técnicas de la criminalística que se realizan de manera sistemática mejorando la capacidad de respuesta ante casos donde se ven involucrados dispositivos digitales y aumentando la probabilidad de éxito en procedimientos judiciales.

Informática Forense: La informática forense, también conocida como cómputo forense, computación forense, análisis forense digital o análisis forense informático, es la disciplina encargada de IDENTIFICAR, PRESERVAR, ANALIZAR Y PRESENTAR evidencias digitales que pueden servir como prueba en un proceso judicial. (Casey, 2011).

Evidencia Digital: Información de valor probatorio almacenado en dispositivos electrónicos.

Criminalística: La criminalística es la disciplina que aplica fundamentalmente los conocimientos, métodos y técnicas de investigación de las ciencias naturales en el examen de material sensible significativo relacionado con un presunto hecho delictuoso, con el fin de determinar, en auxilio de los órganos encargados de procurar y administrar justicia, su existencia, o bien reconstruirlo y señalar y precisar la intervención de uno o varios sujetos en el mismo. (González, 2021).

Modelo: Es la representación simplificada de la realidad.

2. METODOLOGÍA

La presente investigación tiene un enfoque mixto debido a que se combinan aspectos cualitativos y cuantitativos para obtener una visión completa y validada del protocolo de actuación.

Para tal efecto se aplica la metodología de la Ingeniería de Sistemas enmarcadas en las siguientes fases:

- Formulación de los objetivos del modelo.
- Análisis del sistema.
- Síntesis del sistema.
- Verificación del modelo.
- Validación del modelo.
- Inferencias del modelo

Al mismo tiempo considerar la Teoría General de Sistemas como metateoría que permite analizar, estudiar el sistema y construir el modelo.

2.1 Aplicación de la metodología de la Ingeniería de Sistemas

Para el modelo se aplican las fases correspondientes:

2.1.1 Formulación de los objetivos del modelo

Proponer un conjunto de procedimientos estandarizados para mejorar la eficiencia y efectividad de la respuesta ante casos que involucran Dispositivos Digitales, asegurando la integridad de las evidencias y minimizando el tiempo de recuperación.

2.1.2 Análisis del sistema.

Esta fase consiste en identificar los componentes del sistema y sus relaciones entre ellos. Para tal efecto se aplica la Teoría General de Sistemas identificando entrada, proceso y salida del sistema:

Entrada:

Recursos físicos o tangibles, tecnológicos: herramientas físicas (hardware) forenses, herramientas de criminalística (kit de criminalística).

Recursos intangibles: herramientas software forenses, indicios, evidencias, pruebas, delitos informáticos, normativa judicial, código penal, cadena de custodia, Informes Técnicos, Dictamen Pericial.

Recursos humanos: Juez asignado al caso, fiscal asignado al caso, abogados, criminalista de campo, perito informático, consultor técnico, funcionario policial asignado al caso, imputado, sospechoso, víctima.

Recursos económicos: Honorarios, compra de licencias de software, adquisición de kit forense, adquisición de recursos tecnológicos necesarios, costos fijos, variables, mantenimiento, etc.

Proceso:

Aplicación de la metodología de informática forense (Identificación, Preservación, Análisis y Presentación) en combinación con la criminalística, protocolo que se debe seguir frente a un delito informático o casos que involucran dispositivos digitales, con la intervención de especialistas involucrados en el área, con los recursos físicos tangibles e intangibles disponibles, en el marco de las leyes que regulan los delitos informáticos. Como se ve en la figura 1:

Figura 1: Metodología de la Informática Forense
Fuente: Elaboración propia

Salida:

Presentación del Informe Técnico Pericial o Dictamen Pericial en instancias judiciales.

2.1.3 Síntesis del sistema

Consiste en integrar los componentes y relaciones identificados durante el análisis del sistema para crear un modelo coherente que cumpla con los objetivos establecidos.

Para el modelo que se propone se toman en cuenta las técnicas de criminalística.

Criminalística	**Fases de la Informática Forense**
Protección de la escena de los hechos • Observación de la escena • Fijación • Narración • Fotos y Dibujos de croquis, Planimetría, Señalización de evidencias • Rastreo de evidencias • Hipótesis Criminalística Colecta y embalaje de evidencias • Cadena de custodia de evidencias Pericias. Trabajo en Laboratorio • Informes periciales	**Identificación** • **Protección de la escena de los hechos** • **Fijación** **Preservación** • Rastreo • Colecta • Adquisición • Embalaje Físico • Embalaje Lógico • Cadena de Custodia **Análisis** **Presentación** • Informe Técnico Pericial • Dictamen Pericial.

Tabla 1: Relación de Técnicas de Criminalística con las Fases de la Informática Forense

Con base en la metodología de la informática forense y las técnicas empleadas por expertos en investigación criminalística se propone el modelo de la figura 2.

Los componentes del modelo que se propone en la figura 2. se desglosan en la tabla 2, además de las técnicas de la criminalística conocidas por el Personal Policial

(Laboratorio Criminalístico de la FELCC, FELCV e IITCUP) o del Instituto de Investigaciones Forenses (IDIF).

De acuerdo a la metodología de la informática forense, es posible dividir las fases en dos momentos: en el lugar del hecho donde puede realizarse la identificación y preservación, estas fases deben ser manejadas adecuadamente por el personal Policial o el Equipo Multidisciplinario, deben aplicar las técnicas y conocimientos de criminalística para identificar elementos de juicio, por otro lado el perito informático con sus conocimientos técnicos debe estar a cargo de la protección de la Evidencia digital.

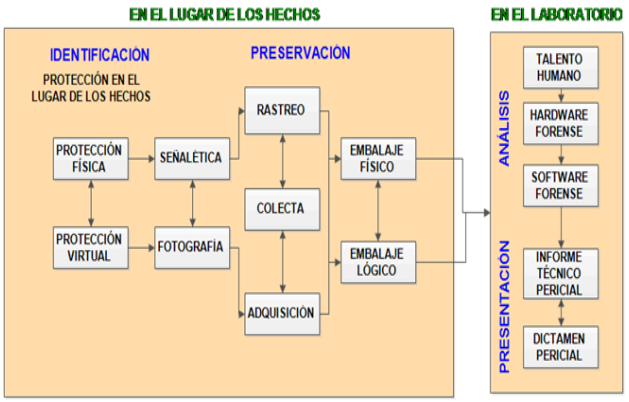

Figura 2: Modelo de Informática Forense con base en Criminalística
Fuente: Elaboración propia

2.1.4 Verificación del modelo

La verificación del modelo incluye etapas de pruebas y revisiones por expertos en informática forense, con el propósito de asegurar que el modelo cumple con las normativas legales antes de la implementación en un entorno real. Al mismo tiempo analizar la funcionalidad del modelo a nivel práctico y teórico.

La etapa de pruebas permitirá observar cómo el equipo multidisciplinario conformado por el fiscal del caso, perito informático, personal de la policía aplican los nuevos procedimientos en un entorno real frente a diversos tipos de incidentes cibernéticos.

2.1.5 Validación del modelo

La validación del modelo conceptual de informática forense basado en criminalística debe asegurar el cumplimiento del objetivo planteado en esta investigación aplicado en un entorno realista, cabe mencionar que es necesario la capacitación del personal que estará involucrado en el equipo de respuesta ante cualquier.

incidente y evaluar la eficiencia en el manejo de incidentes para contribuir a la integridad de las investigaciones.

2.1.6 Inferencias del modelo

Debe permitir mejoras continuas del modelo, el modelo se debe adaptar a nuevos desafíos y aumentar su efectividad y eficiencia.

3. RESULTADOS

El modelo de informática forense basado en criminalística se constituye en un procedimiento sistemático o protocolo de actuación para enfrentar incidentes que involucran evidencia digital, coadyuvando en la resolución efectiva de casos.

Discusión

El modelo propuesto exige que el especialista en informática forense conozca 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 o equipo de respuesta que acude a la escena de los hechos.

4. CONCLUSIONES

Es importante señalar que 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. El modelo propuesto en este artículo cumple una función jurídica que contribuye en la resolución de un caso legal de orden tecnológico, el modelo vincula los conocimientos de criminalística e informática forense para obtener un protocolo de actuación y pueda ser aplicado por un equipo multidisciplinario o equipo de respuesta para llevar a cabo la investigación del hecho delictivo, quienes tendrán la tarea de no perder ningún detalle desde la identificación del lugar del hecho hasta la lectura del dictamen por parte del perito informático, lo que permitirá llevar al convencimiento del juez de la culpabilidad o inocencia de una persona. 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.

REFERENCIAS

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the Internet*. Academic Press.

Hannover, C. (2016, marzo 13). Delitos informáticos carecen de atención oportuna y capaz. *Página Siete*. http://www.paginasiete.bo/sociedad/2016/3/13/delitos-informaticos-carecen-atencion-oportuna-capaz-89688.html

Ministerio de Justicia. (2010). *Código Penal y Código de Procedimiento Penal* (pp. 102–103). Editorial Temis.

Ministerio del Interior del Perú. (2020). *Manual para el recojo de la evidencia digital*. https://www.gob.pe/institucion/mininter/informes-publicaciones/1254510

Rosales, G. (2016). *La informática forense trabaja en Bolivia con tecnología propia*.