MODELO DE INFORMATICA FORENSE BASADO EN CRIMINALÍSTICA

M.Sc. Ing. 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
Acreditado por el
Órgano Judicial de Bolivia
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 y protocolos.*

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, videos, 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. (Gonzalez, 2021)

Modelo: Es la representación simplificada de la realidad.

2. MATERIALES Y MÉTODOS

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.

Aplicación de la metodología de la Ingeniería de Sistemas

Para el modelo se aplican las fases correspondientes:

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.

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.

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
Fuente: Elaboración propia

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.

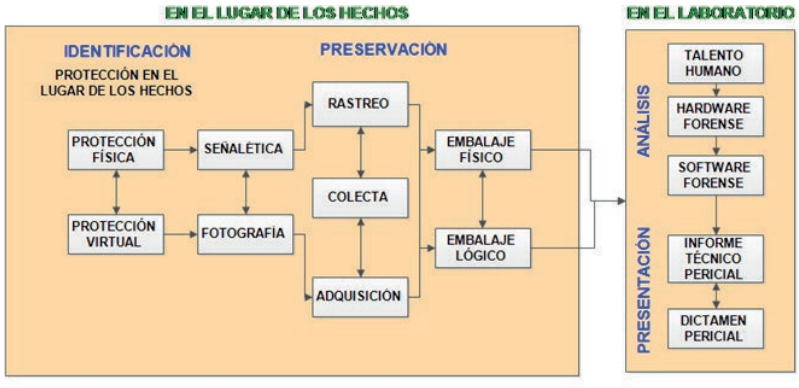

Figura 2: Modelo de Informática Forense con base en Criminalística
Fuente: Elaboración propia

EN LA ESCENA DEL HECHO							EN LABORATORIO				
IDENTIFICACIÓN		PRESERVACIÓN					ANÁLISIS			PRESENTACIÓN	
Está a cargo del equipo multidisciplinario, el objetivo es evitar la contaminación de la escena del hecho.		Permite la obtención de indicios y elementos probatorios para confirmar o refutar la hipótesis, se debe tener cuidado en mantener la autenticidad e integridad de las evidencias. Garantizar la integridad de las evidencias en el tiempo, tomando en cuenta la característica del contenedor donde se va almacenar.					Esta fase requiere de un protocolo, tecnología hardware y software disponible en un laboratorio de informática forense, puede durar tiempo y tiene que ver con el objeto de la investigación y lo hace el perito designado por la autoridad competente. El análisis de las evidencias se debe hacer en el IDIF, el ITCUP o peritos especializados del órgano judicial ODJN.			Documento especializado que redacta el perito informático al finalizar la investigación, incluye todo el procedimiento realizado y los medios que se han utilizado en las diferentes fases de la investigación forense.	
PROTECCIÓN DE LA ESCENA	FIJACIÓN	RASTREO	COLECTA	ADQUISICIÓN	VIRTUAL	FISICA	RECURSOS HUMANOS	RECURSOS FISICOS	RECURSOS TECNOLÓGICOS	INFORME TÉCNICO PERICIAL	DICTAMEN PERICIAL
Proteger la escena del crimen, puede ser una infraestructura tecnológica física, virtual, abierta o cerrada	Debe permitir un estudio posterior, ya que un proceso penal puede durar mucho tiempo.	Identificar elementos que puedan aportar evidencias en la investigación.	Extracción de evidencias y elementos que si aporten para la investigación, incautación de equipos físicos.	Recopilación lógica de información, duplicación de discos duros, considerando la volatilidad de información	Obtención de imágenes forenses de los elementos secuestrados, generación de hashes MD5 o SHA.	se debe considerar: la humedad, estática, magnética y además marcar con códigos de identificación cada evidencia	Peritos informáticos que tengan conocimientos técnicos científicos, en protocolos de actuación frente a delitos informáticos, o casos que involucren evidencia digital.	Infraestructura con un diseño estructural para un laboratorio de informática forense.	Software y hardware forenses (libre o de paga).	Documento que aporta información técnica, uso de herramientas forenses y extracción digital.	Documento que debe aportar a los miembros del tribunal las conclusiones y procedimientos del trabajo pericial.
VIRTUAL	FOTOGRAFIA FORENSE	DISPOSITIVOS DE ALMACENAMIENTO									
Evitar que unidades de procesamiento o sigan con el flujo de información.	Fotografías o filmación de la escena del hecho.	DISPOSITIVOS DE PROCESAMIENTO									
FISICA	SEÑALETICA	DISPOSITIVOS DE TRANSFERENCIA									
Proteger la infraestructura tecnológica.	Señalar con numeros las evidencias, que se encuentran en la escena del hecho										

Tabla 2: Descripción de los Componentes del Modelo
Fuente: Elaboración propia

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 asignado al caso, perito informático y personal de la policía boliviana aplican los nuevos procedimientos en un entorno real frente a diversos tipos de casos relacionados con evidencia digital.

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 caso relacionado con evidencia digital y evaluar la eficiencia en el manejo de casos para contribuir a la integridad de las investigaciones.

Inferencias del modelo

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

Estadística de Cibercrimen en Bolivia

De acuerdo a información recopilada del sitio web oficial de ODIB (Observatorio de Delitos Informáticos en Bolivia) relacionados a casos que involucra evidencia digital, con base en la tabla 2 se muestra en la figura 3 hallazgos estadísticos significativos en relación con los delitos informáticos en el Estado Plurinacional de Bolivia. Entre los principales hallazgos se destacan tres tipos de delitos que muestran una prevalencia notable: "Fraude o Estafa Informática", "Amenazas" y "Grooming". Estos resultados reflejan una tendencia preocupante en el aumento de la incidencia de delitos cibernéticos en el país. (Díaz, 2024)

#	TIPO DE CASO/DELITO	LP	CBBA	SC	El Alto	OR	PT	BN	PD	CH	TJ	TOTAL
1	Fraude o Estafa Informática	234	147	191	121	52	26	17	9	43	26	**867**
2	Phishing	71	45	58	37	16	8	5	3	13	8	**264**
3	Amenazas	183	115	149	95	41	20	14	7	34	20	**678**
4	Calumnias o Injurias	112	70	91	58	25	12	8	4	21	12	**414**
5	Difusión de Abuso Sexual Infantil	61	38	50	32	14	7	5	2	11	7	**226**
6	Suplantación de Identidad Digital	41	26	33	21	9	5	3	2	8	5	**151**
7	Difusión de Malware	31	19	25	16	7	3	2	1	6	3	**113**
8	Manipulación Informática (Hacking)	51	32	41	26	11	6	4	2	9	6	**188**
9	Sabotaje Informático	31	19	25	16	7	3	2	1	6	3	**113**
10	Grooming (Acoso sexual a menores)	132	83	108	69	29	15	10	5	24	15	**490**
11	Sextorsión y Chantaje	71	45	58	37	16	8	5	3	13	8	**264**
		1017	641	829	528	226	113	75	38	188	113	**3768**

Tabla 2: Casos que involucran evidencia digital en Bolivia
Fuente: https://www.odibolivia.org

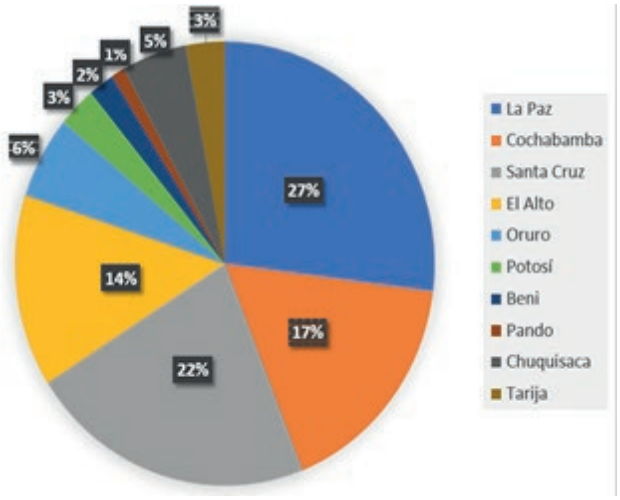

Figura 3: Gráfico de proporción de delitos cibernéticos por departamento
Fuente: https://www.odibolivia.org

Por otra parte, se puede clasificar los casos donde se involucra evidencia digital registrados y diferenciados por rango de edad de las víctimas, se tiene la siguiente tabla 3.

#	TIPO DE CASO/DELITO	Menor de 15	Entre 16 y 21	Entre 22 y 35	Entre 36 y 50	Mayor a 51	TOTAL
1	Fraude o Estafa Informática	121	191	199	217	139	**867**
2	Phishing	5	50	87	71	50	**264**
3	Amenazas	176	190	122	102	88	**678**
4	Calumnias o Injurias	8	99	162	87	58	**414**
5	Difusión de Abuso Sexual Infantil	133	93	0	0	0	**226**
6	Suplantación de Identidad Digital	29	36	41	30	15	**151**
7	Difusión de Malware	20	27	33	23	10	**113**
8	Manipulación Informática (Hacking)	15	32	47	57	38	**188**
9	Sabotaje Informático	11	19	29	34	19	**113**
10	Grooming (Acoso sexual a menores)	270	220	0	0	0	**490**
11	Sextorsión y Chantaje	63	79	50	40	32	**264**
		853	1037	770	659	449	**3768**

Tabla 3: Casos registrados por rango de edad de las víctimas
Fuente: https://www.odibolivia.org

3. RESULTADOS Y DISCUSIÓN

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.

El modelo propuesto exige que el especialista en informática forense conozca aspectos legales y de investigación criminalística técnico científica 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 al lugar 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.

BIBLIOGRAFIA

[1] Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.

[2] Díaz, C. R. (2024). Informe sobre Cibercrimen en el Estado Plurinacional de Bolivia. La Paz.

[3] Gonzales, R. M. (2021). Criminalística, Principios, Técnicas y Métodos. Mexico: Porrúa.

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

[5] MinisteriodeJusticia. (2010). Código Penal y Codigo de Procedimiento Penal. En Ministeriode-Justicia, Código Penal y Codigo de Procedimiento Penal (págs. 102, 103). La Paz: Temis.

[6] Manual Para el Recojo de la Evidencia Digital, Ministerio del Perú, 2020

[7] Rosales G (2016) la-informatica-forense-trabaja-en-bolivia-con-tecnologia-propia

SOBRE LOS AUTORES:

Elizabeth Mejía García: 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 programas de diplomado en la Universidad Nacional "Siglo XX", 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.

Álvaro Rodrigo Calle Maydana: Perito en Informática Forense acreditado por el Órgano Judicial de Bolivia ODIN con 5 años de experiencia, miembro de la Red Latinoamericana de Informática Forense REDLIF , miembro de la Sociedad Científica de Ciencias Forenses Tarija, Diplomado en Riesgos Digitales, Diplomado en Educación Superior, Certificación en la ISO 27001, Investigador Privado por el Instituto Internacional CENCASI, certificaciones en Certified Computer Examiner - CCE, Riesgos Digitales, Seguridad Informática , egresado de la Escuela Industrial Superior "Pedro Domingo Murillo ", Técnico Superior en Ciencias Policiales de la Universidad Policial Mariscal Antonio José de Sucre.

Fig 5. Fotografía de presentación de la ponencia