UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMÁTICA

TESIS DE GRADO

"MÉTODO INFORMÁTICO FORENSE PARA EL MANEJO ADECUADO DE LA EVIDENCIA DIGITAL Y SU ADMISIBILIDAD EN SITUACIONES JURÍDICAS EN BOLIVIA"

PARA OPTAR AL TITULO DE LICENCIATURA EN INFORMÁTICA
MENCIÓN: INGENIERIA DE SISTEMAS INFORMATICOS

AUTOR: XIMENA EUGENIA PATIÑO BUSTILLOS
TUTOR: MSC. LIC. MARIO LOAYZA MOLINA
REVISOR: LIC. GROVER ALEX RODRÍGUEZ RAMIREZ

LA PAZ – BOLIVIA
2009

DEDICATORIA

A Dios por ser el Amor, el Camino y la Luz que guía mis pasos, por darme las fuerzas para seguir adelante, bendecir mi vida a diario y por que siempre lo llevo en mi corazón.

A nuestra Virgen María por que con su manto bendito siempre nos protege de todo mal.

A mis Padres Enrique y Eva a quienes adoro con todo mí ser, por el amor y la confianza que me brindan día a día, por su constante dedicación, por las muestras de cariño, por su buen ejemplo y por haber trabajado arduamente a lo largo de sus vidas en beneficio mío y de mi familia.

A mis hermanos Ingrid y Edwin por ser mis compañeros en mi diario vivir, por los consejos y apoyo que me brindan.

A todos mis familiares: abuelos, tíos, primos y sobrinos, por fortalecer los lazos que nos une como familia y por el cariño que me tienen.

A Oscar por que con su amor, comprensión, paciencia, apoyo y cariño, me motiva a seguir adelante.

Gracias.

AGRADECIMIENTOS

A Dios por permitirme existir y por no dejarme desfallecer en los momentos más difíciles.

Al Lic. Mario Loayza Molina, mi tutor, por su colaboración, apoyo y consejos, para que se haga realidad ésta tesis.

Al Lic. Grover Rodríguez Ramírez, mi revisor, por las sugerencias, correcciones y el tiempo dedicado a mi tesis, quien me brindó su apoyo constantemente.

Al Ing. Gustavo D. Presman y al Ing. Leopoldo Sebastián Gómez (Peritos en Informática Forense de la Provincia de Neuquén - Argentina), por la colaboración prestada sin importar las distancias.

Al Lic. Daniel Guisbert S., quien me colaboró en el aspecto legal, por compartir sus conocimientos y asesorarme en el campo del Derecho Informático.

A cada uno de los docentes de la Carrera de Informática, por brindarnos enseñanza con dedicación y desinterés. A los administrativos y bibliotecarios por brindarnos su amistad, cordialidad y calidez de persona que los caracteriza.

A mis amig@s, quienes me ofrecieron una amistad y cariño sincero: Paola, Verónica, Giovanna, Teresa, Adelaida, Gisel, Yadranka, Lizeth, Chano, Daniel, Jaime, Milton, Robert y a otros amigos de la carrera.

A todos y cada uno de los miembros de la “Fraternidad Tobas Jaguar de la Carrera de Informática”, por las alegrías, emociones y experiencias que viví gracias a la confianza que me dieron al elegirme “Ñusta 2008” de ésta fraternidad, púes con sus muestras de afecto y detalles para conmigo, me colmaron de mucha felicidad y esto me motivó más aún a seguir adelante y luchar por lo que quiero.

RESÚMEN

En nuestro país ya se realizan de manera empírica investigaciones sobre posibles ilícitos donde se ven involucrados elementos informáticos.

Al ser la informática forense una disciplina que no tiene muchos años siendo practicada en nuestro medio, se cometen errores al momento de manejar la evidencia digital (parte fundamental en investigaciones de éste tipo), lo cual resta credibilidad al ser tratada de manera inadecuada y por ende es propenso a ser inadmisible en un proceso penal.

Debido a lo explicado anteriormente, es que en la presente Tesis de Grado se desarrolla y propone un Método Informático Forense que permita manejar adecuadamente la evidencia digital, mantener de los elementos probatorios la autenticidad, confiabilidad, suficiencia y conformidad con la legislación vigente en nuestro país; estos cuatro conceptos son fundamentales para lograr que la evidencia sea admisible.

Para tal efecto se desarrollan procedimientos para la identificación, adquisición, preservación y análisis de la evidencia digital, además de un procedimiento para que la evidencia digital sea permitida legalmente, con la finalidad de precautelar la integridad de la misma y hacer que ésta sea admisible en un proceso jurídico en nuestro país.

INDICE DE CONTENIDO

CAPÍTULO 1 MARCO PRELIMINAR

CAPITULO 2 MARCO DE REFERENCIA

INDICE DE FIGURAS Y TABLAS

CAPÍTULO 1
MARCO PRELIMINAR

Capítulo 1

MARCO PRELIMINAR

1.1 Introducción

Actualmente en Bolivia, ya se hacen presentes las investigaciones sobre posibles ilícitos que involucran el análisis de elementos informáticos, lo que implica el tratar adecuadamente la evidencia digital, partiendo por el principio de e_locard (1). Poseer un conocimiento profundo de los desafíos que se plantean en el campo de la Informática Forense y contar con un marco legal adecuado, apoyaría de gran manera en el esclarecimiento de delitos cometidos bajo soporte informático, ya que es evidente la existencia e incremento de delitos informáticos en nuestro país (ver Anexo A).

Los hallazgos digitales -ya sea como prueba o como medio para dilucidar la maniobra delictiva- hace casi imprescindible considerarlos durante una investigación judicial. Hay una línea de pensamiento que considera que "la gran mayoría de los ilícitos informáticos pueden encuadrarse en los tipos penales tradicionales, en la medida en que sistemas computarizados sean utilizados como medio, instrumento, herramienta u objeto de aquellos" (2), por ejemplo la pornografía infantil, los fraudes y el robo de propiedad intelectual.

Las actividades delictivas con alta tecnología -en particular los medios informáticos- presentan un importante desafío a los operadores judiciales durante el desarrollo de una investigación, quienes apoyados en los conocimientos de profesionales informáticos forenses pretenden esclarecer éste tipo de hechos. Es evidente que durante una investigación lo que más se quiere es minimizar cualquier error que pueda hacer fracasar la consecución de elementos probatorios.

---

1 e_locard Principio sobre el intercambio entre dos cuerpos que entran en contacto, se afirma que ambos intercambian algo en el proceso Cuando dos dispositivos electrónicos se comunican intercambian datos siguiendo un protocolo, el rastro queda almacenado y dependiendo del tipo de almacenamiento se lo puede encontrar posterior al proceso de intercambio

2 Rinaldi, S , "Delitos informáticos, perfil criminológico del hacker, especial referencia a los delitos de contenido económico y normativa aplicable", Primeras Jornadas Latinoamericanas de Derecho Informático, Mar del Plata, (2001)

Existen numerosas razones que pueden llevar a cometer errores en el manejo de la evidencia digital, ésto a consecuencia de la ausencia de procedimientos y métodos formales en nuestro medio.

Al cometer esos errores, disminuye la posibilidad del esclarecimiento de éste tipo de delitos, ya que es posible que la evidencia digital recabada en la escena del hecho quede descartada (anulada).

Es por tal situación que en la presente tesis se propone un método informatico forense que permita el manejo adecuado de la evidencia digital, que debe ser considerado por los profesionales informáticos para una mejor concepción del alcance, duración y limitaciones en la tarea de determinación de la evidencia digital. De tal forma que permita mejorar, sistematizar y estimar las tareas de investigación de actividades delictivas sobre material informático, a fin de facilitar la repetición de lo realizado.

Éste trabajo de investigación es elaborado, acudiendo al conocimiento de profesionales especialistas en Informática Forense, además de trabajos de investigación, artículos científicos, prácticas internacionales y demás documentación.

1.2 Antecedentes

En la actualidad se carece de metodologías, procedimientos y métodos de informática forense que permitan realizar un manejo adecuado de la evidencia digital de forma explícita y altamente aplicativa en nuestro medio.

El avance de la tecnología lleva un ritmo acelerado y nuestra legislación penal, no puede receptar con facilidad estos adelantos tecnológicos dando lugar a situaciones de duda. En nuestro país sólo han sido objeto de tipificación en forma parcial mediante leyes que regulan penalmente las conductas ilícitas relacionadas con los delitos informáticos en sólo dos artículos del Código Penal (ver Anexo B).

En el articulo científico denominado "EVIDENCIA DIGITAL EN EL CONTEXTO COLOMBIANO" [Torres et al., 2003], se nombra un procedimiento forense para el manejo de investigaciones, en el que se dá pautas para el tratamiento de la evidencia digital, se establecen cinco etapas: planeación, recolección, aseguramiento, análisis y presentación de la evidencia digital, pero no es muy clara y deja muchas dudas para el lector, como si hablar de éste tema fuese un secreto.

En algunas publicaciones de revistas científicas dicen que en la informatica forense se debe aplicar los métodos referentes a ésta, pero no dan a conocer en que consisten esos métodos.

Por ejemplo en el artículo científico "Informática Forense" [Reino, 2007], indica que "*la metodología aplicada debe ser conocida, de forma que otros investigadores, utilizando los mismos métodos, puedan llegar a conclusiones similares*", pero realizando investigaciones no se tiene conocimiento de éstos métodos y metologías a las que hace referencia el autor.

1.3 Planteamiento del problema

Se cometen errores en el manejo de la evidencia digital, lo que no garantiza la autenticidad, confiabilidad, suficiencia, conformidad con leyes y reglas de justicia de los elementos probatorios, en consecuencia la evidencia digital llega a ser inadmisible en un proceso jurídico, debido a que dicha evidencia no es adquirida, identificada, preservada y analizada de manera adecuada.

Al ser inadmisible la evidencia digital en el proceso judicial, no se tendrán las pruebas necesarias para que juzguen al delincuente y lo castiguen por sus conductas impropias, y quedarán sin esclarecimiento este tipo de hechos, lo cual alentará al incremento de delitos informáticos.

1.4 Formulación del problema

¿Con un Método Informático Forense se puede lograr que exista un manejo adecuado de la evidencia digital, que permita garantizar de los elementos probatorios la autenticidad, confiabilidad, suficiencia, conformidad con leyes y reglas de justicia, y así hacer que ésta evidencia sea admisible en un proceso jurídico?

En general, las legislaciones y las instituciones de justicia han fundado sus reflexiones sobre la admisibilidad de la evidencia en cuatro conceptos: "Autenticidad", "Confiabilidad", "Suficiencia", "Conformidad con las leyes y reglas de la administración de justicia" [Cano, 2003a].

Autenticidad: satisfacer a una corte en que los contenidos de la evidencia no han sido modificados, la información proviene de la fuente identificada, la información externa es precisa.

Confiabilidad: debe ser posible relacionarla con el incidente. No debe haber ninguna duda sobre los procedimientos seguidos y las herramientas utilizadas para su recolección, manejo, análisis y posterior presentación en una corte.

Suficiencia: debe por si misma y en sus propios términos mostrar el escenario completo, y no una perspectiva de un conjunto particular de circunstancias o eventos.

Conformidad con las leyes y reglas de la administración de justicia: Cuando se tiene acceso a la evidencia digital por medios no autorizados y no hay vías para probar su autenticidad, confiabilidad y suficiencia, los elementos aportados carecerán de la validez requerida y serán tachados de ilegales. La evidencia obtenida de esta manera no ofrece formas para comprobar las posibles hipótesis que, sobre el caso, se hayan efectuado, dadas las irregularidades que enmarcan su presentación.

1.5 Objetivos

1.5.1 Objetivo General

Desarrollar y proponer un método informático forense que permita manejar adecuadamente la evidencia digital, mantener de los elementos probatorios la autenticidad, confiabilidad, suficiencia, conformidad con leyes y reglas de justicia, y así garantizar la admisibilidad de la misma en situaciones jurídicas.

1.5.2 Objetivos Específicos

- ✓ Plantear un procedimiento para identificar la evidencia a secuestrar
- ✓ Desarrollar un procedimiento para adquirir la evidencia digital
- ✓ Formular un procedimiento para preservar la evidencia digital
- ✓ Proponer un procedimiento para analizar la evidencia digital
- ✓ Dar a conocer un procedimiento para que la evidencia digital sea permitida legalmente

1. 6 Hipótesis

El método informático forense, garantiza la admisibilidad de la evidencia digital en situaciones jurídicas en nuestro país, si existe un manejo adecuado de la evidencia digital.

1.7 Justificación

1.7.1 Justificación Teórica

Éste trabajo de investigación será un complemento teórico para la aplicación de la informática forense en nuestro país, referente al manejo adecuado de la evidencia digital, estableciendo un método que sea aplicable y de fácil comprensión, por que en la actualidad se carece del mismo.

1.7.2 Justificación Práctica

1.7.2.1 Justificación Social

Al ser la informática forense una disciplina que recién está siendo practicada en nuestro país (de forma empírica), es necesaria la formación de profesionales en ésta área, por nuestra Casa Superior de Estudios la Universidad Mayor de San Andrés específicamente por la Carrera de Informática perteneciente a la Facultad de Ciencias Puras y Naturales, para lo cual se necesitará de manera imprescindible metodologías, métodos y materiales bibliográficos en las cuales sustentarse, para la aplicación y enseñanza de ésta especialidad.

Los beneficios sociales son muy amplios, desde coadyuvar en la formación de profesionales con el adecuado conocimiento sobre el manejo de la evidencia digital en la aplicación de la informatica forense, hasta generar una mayor confianza en dichos profesionales, pues con éste método informático forense se motivará al manejo adecuado de la evidencia digital, lo cual coadyuvara a la reducción de la posibilidad de cometer errores en su manejo y en alguna medida garantizará la admisibilidad de la misma en situaciones jurídicas, se podrá tomar decisiones concretas en un determinado momento que se esté trabajando con evidencia digital.

Además conllevará en una correcta investigación del hecho cometido, que posibilitará el castigo de conductas impropias y en consecuencia nos llevaría a mejorar la prevención de estas conductas dado el carácter disuasivo que se logra cuando las investigaciones criminales llegan al castigo del delincuente.

1.7.2.2 Justificación Económica

Económicamente tiene un gran impacto, puesto que cuando se investiga delitos informáticos, en la mayoría de los casos se espera un resarcimiento de daños a las victimas (en montos económicos elevados) dispuestos por la autoridad competente.

Si el profesional informático comete errores en el manejo de la evidencia digital, será inadmisible la misma, lo que no permitirá que se utilice de prueba y si tomamos en cuenta que era la única prueba el delito cometido, éste quedará sin esclarecimiento y en consecuencia no se sancionará a los responsables de tal ilícito, además que la remuneración económica en cada nuevo proceso será inferior, debido a que el prestigio del mismo estará en descenso, pero con éste método informático forense, podrá realizar una investigación donde se maneje adecuadamente la evidencia digital, pues ya tendrá una base en la cual fundamentarse y de ésta manera logrará garantizar la admisibilidad de la evidencia en situaciones jurídicas, lo que posibilita el esclarecimiento del delito cometido, en consecuencia su prestigio se ira elevando cada vez mas al igual que sus ingresos económicos por su desempeño profesional.

Si cuantificamos el costo de éste método informático forense y los beneficios que obtendremos con el mismo, claramente se aprecia que el beneficio es mayor al costo, sin dejar de tomar en cuenta que existirían muchos beneficiados.

En otros países como México, los fraudes en cuentas bancarias, son denunciadas como demandas mercantiles (para que el banco les regrese su dinero) o demandas penales (para castigar al responsable del delito) [Velásquez, 2008], una buena aplicación del método informático forense lograría el esclarecimiento del delito y por ende la posible devolución del dinero sustraído.

1.7.2.3 Justificación Tecnológica

Las herramientas tecnológicas que se utilizan en Informática Forense, están al alcance de los entendidos en ésta materia, el proponer éste método informático forense para el manejo adecuado de la evidencia digital, servirá para poder ser utilizado por profesionales informáticos, ingenieros de sistemas, consultoras de auditoria informática, por la FELCC (Fuerza Especial de Lucha Contra el Crimen) y otras personas interesadas en ésta disciplina.

1.8 Alcances y Limites

Se elaborará un método informático forense para el manejo adecuado de la evidencia digital, detallada y formal. Se explicará de la mejor manera la aplicabilidad del mismo, el cual permitirá al informático contar con un instrumento específico, que facilite emitir resultados con respecto a investigaciones realizadas, en delitos cometidos con soporte informático

El cual contará con procedimientos para:

- Identificar la evidencia a secuestrar
- Adquirir evidencia digital
- Preservar la evidencia digital
- Analizar la evidencia digital
- Asegurar que la evidencia digital sea permitida legalmente

Se dará a conocer las características técnicas mínimas que deben cumplir las herramientas forenses (ver Anexo D) para que la evidencia adquirida y/o analizada por ellas sea confiable, pero no se explicará cómo se trabaja con cada herramienta, ya que no es el propósito de ésta tesis.

Éste método informático forense está propuesto tomando en cuenta la perspectiva de ser aplicado en el campo de Computer forensics (computación forense) y no así en digital forensics (forensia digital) o network forensics (forensia en redes), que también son partes de la Informática Forense.

El método informático forense para el manejo adecuado de la evidencia digital y su admisibilidad en situaciones jurídicas en Bolivia, se enmarca sólo hasta la admisibilidad de la evidencia digital en un proceso jurídico; además que no asegura la admisibilidad de la evidencia digital, en el caso de que existan errores humanos (descuidos u otros) en el manejo de la evidencia digital.

CAPÍTULO 2
MARCO DE REFERENCIA

Capítulo 2

MARCO DE REFERENCIA

2.1 Marco Teórico

2.1.1 Informática Forense

La informática forense se define como una rama de la informática que se encarga de recolectar y/o recopilar información valiosa desde sistemas informáticos (redes, ordenadores, soportes magnéticos, ópticos, etc.) con distintos fines, sirviendo de apoyo a otras disciplinas o actividades, como son las labores de criminalística e investigaciones. Estas evidencias que permite descubrir diferentes datos sirven, por ejemplo, para condenar o absolver a algún imputado. La idea principal de este tipo de informática es colaborar con la criminalística [Restrepo, 2007].

Se reconoce a Dan Farmer y Wietese Venema, como los pioneros de la informática forense, actualmente Brian Carrier es probablemente uno de los expertos mundiales en el tema.

Esta rama tuvo su origen en 1984 cuando el FBI y otras agencias de Estados Unidos comenzaron a desarrollar programas para examinar evidencia computacional.

La Informática Forense recolecta y utiliza la evidencia digital para casos de delitos informáticos y para otro tipo de crímenes usando técnicas y tecnologías avanzadas. Un experto en informática forense utiliza estas técnicas para descubrir evidencia de un dispositivo de almacenaje electrónico. Los datos pueden ser de cualquier clase de dispositivo electrónico como discos duros, discos compactos, discos flexibles, cintas de respaldo, computadores portátiles, memorias extraíbles, archivos y correos electrónicos.

La mayoría de los usuarios piensan que al borrar un archivo se quitará totalmente la información del disco duro. En realidad se quita solamente el archivo de localización, pero el archivo real todavía queda en su computadora.

La Informática Forense se puede utilizar para descubrir un fraude, uso no autorizado de computadoras, una violación de políticas de compañías, historial de chats, archivos y navegación o cualquier otra forma de comunicaciones electrónicas.

2.1.1.1 Definiciones

Existen múltiples definiciones a la fecha sobre el tema forense en informática [Mckemmish, 1999]. Una primera revisión nos sugiere diferentes términos para aproximarnos a este tema, dentro de los cuales se tienen: computer forensics (computación forense), digital forensics (forensia digital), network forensics (forensia en redes), entre otros. Este conjunto de términos puede generar confusión en los diferentes ambientes o escenarios donde se utilice, pues cada uno de ellos trata de manera particular o general temas que son de interés para las ciencias forenses aplicadas en medios informáticos.

2.1.1.2 Clasificación

Computer forensics, cuya traducción por lo general se hace como computación forense. Esta expresión podría interpretarse de dos maneras: i) Disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso. ii) Como la disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos.

Estas dos definiciones no son excluyentes, sino complementarias. Una de ellas hace énfasis en las consideraciones forenses y la otra en la especialidad técnica, pero en últimas ambas procuran el esclarecimiento e interpretación de la información en los medios informáticos como valor fundamental, uno para la justicia y otro para la informática.

Cuando se habla de network forensics, forensia en redes, estamos en un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular.

Esta conjunción de palabras establece un profesional que entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción.

A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, que en equipos particulares, es poco frecuente.

Digital forensics, forensia digital, trata de conjugar de manera amplia la nueva especialidad. Podríamos hacer semejanza con computación forense, al ser una forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos, de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática [Cano, 2003b].

2.1.2 Delitos Informáticos

Los delitos informáticos, en general, son aquellos actos delictivos realizados con el uso de computadoras o medios electrónicos, cuando tales conductas constituyen el único medio de comisión posible –o el considerablemente más efectivo-, y los delitos en que se daña estos equipos, redes informáticas, o la información contenida en ellos, vulnerando bienes jurídicos protegidos [Wikipedia, 2008].

Existen dos Clasificaciones de Delitos Informáticos según Julio Téllez Valdés [Caracciolo]:

- ✓ Como instrumento o medio
- ✓ Como fin u objetivo

Todas aquellas conductas criminales que se valen de las computadoras como método, medio o símbolo para cometer un ilícito.

2.1.2.1 Como Instrumentos

Se utilizan a las computadoras para realizar falsificaciones de documentos de uso comercial. Tal es el caso de Recibos de Sueldos, Comprobantes, Escrituras.

2.1.2.2 Como Medios

Son conductas criminales en donde para realizar un delito utilizan una computadora como medio o símbolo.

2.1.2.3 Ejemplos de Delitos como Instrumentos o Medios

- Alteración de Documentación Legal.
- Planeamiento y simulación de delitos convencionales tales como robos, homicidios, fraudes.
- Lectura, sustracción o copiado de información confidencial
- Modificación de datos tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa
- Uso no autorizado de programas.
- Introducción de instrucciones que provocan denegaciones de Servicios totales o parciales

- Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
- Intervención en las líneas de comunicación de datos o teleproceso
- Espionaje
- Terrorismo
- Narcotráfico
- Redes de Pornografía Infantil

2.1.2.4 Como Fin u Objetivos

Son conductas criminales que van dirigidas contra la computadora, sus accesorios o sus programas como entidad física. Es decir que son conductas criminales dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

2.1.2.5 Ejemplos de Delitos como Fin u Objetivos

- Generación o Implementación de Software malicioso que producen el bloqueo total de un sistema.
- Destrucción del Software de los equipos.
- Destrucción Física de la máquina o de sus accesorios.
- Secuestro de soportes magnéticos, ópticos o de cualquier tipo para extorsionar a sus dueños.
- Acceso no autorizado a un sistema o la misma Intercepción de los correos electrónicos.
- Estafas Electrónicas como el Phishing.

2.1.3 Evidencia digital

Es un tipo de evidencia física, esta construida de campos magnéticos y pulsos electrónicos, que pueden ser recolectados y analizados con herramientas y técnicas especiales.

También se puede definir como: Cualquier objeto, archivo, fotografía u otro que tenga estrecha relación o este realizado mediante soporte informático, el cual se encuentre vinculado con algún delito, que posteriormente es recolectado de una escena del hecho [Rosales, 2008].

Se trata de demostrar una entrada, existencia, copia, que haya sido realizado usando medios informáticos, presenta particularidades no conceptuales sino directamente relacionadas con el medio físico que la soporta, el cual al ser electrónico, magnético u óptico puede sufrir alteraciones, modificaciones o simplemente daños permanentes al ser apagado, trasladado, encendido o cualquier otra acción casual o intencionada.

2.1.3.1 Ciclo de vida para la administración de la evidencia digital: [Standards Australia International, 2003]

Diseño de la evidencia:

1. Producción de la evidencia digital
2. Recolección de la evidencia digital
3. Análisis de la evidencia digital
4. Reporte y presentación
5. Determinación de la relevancia de la evidencia digital

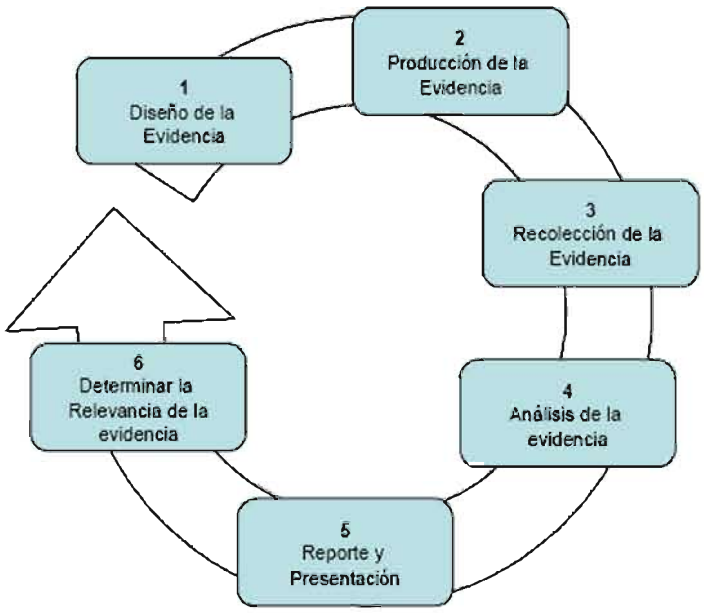


Figura 1. Ciclo de vida de la administración de la evidencia digital

Fuente: Standards Australia International

2.1.3.2 Diseño de la evidencia

Con el fin de fortalecer la admisibilidad y relevancia de la evidencia producida por las tecnologías de información, se detallan a continuación cinco objetivos que se deben considerar para el diseño de la evidencia digital:

a. Asegúrese de que se ha determinado la relevancia de los registros electrónicos, que éstos se han identificado, están disponibles y son utilizables.

b. Los registros electrónicos tienen un autor claramente identificado.

c. Los registros electrónicos cuentan con una fecha y hora de creación o alteración.

d. Los registros electrónicos cuentan con elementos que permiten validar su autenticidad.

e. Se debe verificar la confiabilidad de la producción o generación de los registros electrónicos por parte del sistema de información.

2.1.3.3 Producción de la Evidencia

Esta fase, de acuerdo con el estándar, requiere el cumplimiento de los siguientes objetivos:

a. Que el sistema o tecnología de información produzca los registros electrónicos

b. Identificar el autor de los registros electrónicos almacenados

c. Identificar la fecha y hora de creación

d. Verificar que la aplicación está operando correctamente en el momento de la generación de los registros, bien sea en su creación o modificación.

e. Verificar la completitud de los registros generados

2.1.3.4 Recolección de la Evidencia

El objetivo de esta fase en el ciclo de vida de administración de la evidencia digital es localizar toda la evidencia digital y asegurar que todos los registros electrónicos originales (aquellos disponibles y asegurados en las máquinas o dispositivos) no han sido alterados. Para ello el estándar establece algunos elementos a considerar como:

a. Establecer buenas prácticas y estándares para recolección de evidencia digital

b. Preparar las evidencias para ser utilizadas en la actualidad y en tiempo futuro

c. Mantener y verificar la cadena de custodia

d. Respetar y validar las regulaciones y normativas alrededor de la recolección de la evidencia digital

e. Desarrollar criterios para establecer la relevancia o no de la evidencia recolectada.

2.1.3.5 Análisis de la Evidencia

Una vez se ha recolectado la evidencia, tomado las imágenes de los datos requeridos y su debida cadena de custodia, es tiempo para iniciar el ensamble, análisis y articulación de los registros electrónicos para establecer los hechos de los eventos ocurridos en el contexto de la situación bajo análisis o establecer si hacen falta evidencias para completar o aclarar los hechos.

2.1.3.6 Reporte y Presentación

El profesional a cargo de la investigación es responsable de la precisión y completitud del reporte, sus hallazgos y resultados luego del análisis de la evidencia digital o registros electrónicos. En este sentido toda la documentación debe ser completa, precisa, comprensiva y auditable.

Las prácticas internacionales aconsejan:

a. Documentar los procedimientos efectuados por el profesional a cargo.

b. Mantener una bitácora de uso y aplicación de los procedimientos técnicos utilizados.

c. Cumplir con exhaustivo cuidado con los procedimientos previstos para el mantenimiento de la cadena de custodia.

2.1.3.7 Determinar la relevancia de la evidencia

El estándar en esta fase establece valorar las evidencias de tal manera que se identifiquen las mejores evidencias que permitan presentar de manera clara y eficaz los elementos que se desean aportar en el proceso y en el juicio que se lleve. El objetivo es que el ente que valore las pruebas aportadas observe en sus análisis y aportes los objetos de prueba más relevantes para el esclarecimiento de los hechos en discusión.

En este sentido el estándar sugiere dos criterios para tener en cuenta a saber: [Standards Australia International, 2003]

a. Valor probatorio: que establece aquel registro electrónico que tenga signo distintivo de autoría, autenticidad y que sea fruto de la correcta operación, confiabilidad del sistema.

b. Reglas de la evidencia: que establece que se han seguido los procedimientos, reglas establecidas para la adecuada recolección y manejo de la evidencia.

2.1.4 Admisibilidad de la evidencia digital [Cano, 2003a]

La evidencia digital (representada en todas las formas de registro magnético u óptico generadas por las organizaciones) debe avanzar hacia una estrategia de formalización que ofrezca un cuerpo formal de evaluación y análisis que deba ser observado por el ordenamiento judicial de un país. En general, las legislaciones y las instituciones de justicia han fundado sus reflexiones sobre la admisibilidad de la evidencia en cuatro conceptos [Sommer, 1995][Casey, 2001][IOCE, 2000 cap.6], que a continuación se detallan.

2.1.4.1 Autenticidad

Sugiere ilustrar a las partes que la evidencia ha sido generada y registrada en los sitios relacionados con el caso, particularmente en la escena del posible ilícito o lugares establecidos en la diligencia de levantamiento de evidencia.

Asimismo, la autenticidad es entendida como aquella característica que muestra la *no alterabilidad de los medios originales* y busca confirmar que los registros aportados correspondan a la realidad evidenciada en la fase de identificación y recolección.

En los medios digitales, dada la volatilidad y alta capacidad de manipulación que se presenta en el almacenamiento electrónico. Si bien estas características también son, de alguna manera, inherentes a las vías tradicionales, el detalle se encuentra en que existe una serie de procedimientos asociados con el manejo y control de los

mismos en las organizaciones, mientras que para los registros magnéticos aún no se tiene la misma formalidad.

Verificar la autenticidad de los registros digitales requiere, de manera complementaria, a la directriz general establecida por la organización sobre éstos, el desarrollo y configuración de mecanismos de control de integridad de archivos, es decir, necesita que una arquitectura exhiba mecanismos que aseguren la integridad de los registros y el control de cambios de los mismos.

Al establecer una arquitectura de cómputo con la que se fortalezca la protección de los medios digitales de registro y el procedimiento asociado para su verificación, aumenta sustancialmente la veracidad de las pruebas recolectadas y aportadas. En consecuencia, la información que se identifique en una arquitectura con estas características tendrá mayor fuerza y solidez, no sólo por lo que su contenido ofrezca, sino por las condiciones de generación, control y revisión de los registros electrónicos.

En otras palabras, al contar con mecanismos y procedimientos de control de integridad, se disminuye la incertidumbre sobre la manipulación no autorizada de la evidencia aportada y se concentra el proceso en los hechos y no en errores técnicos de control de la evidencia digital bajo análisis.

2.1.4.2 Confiabilidad

Es otro factor relevante para asegurar la admisibilidad de la misma. La confiabilidad nos dice si, efectivamente, los elementos probatorios aportados vienen de fuentes que son creíbles y verificables y que sustentan elementos de la defensa o del fiscal en el proceso que se sigue. En medios digitales podríamos relacionar este concepto a ¿cómo se recogen y analizan las evidencias digitales?, son preguntas cuyas respuestas buscan demostrar que poseen una manera confiable para ser identificados, adquiridos y verificados.

Cuando logramos que una arquitectura de cómputo ofrezca mecanismos de sincronización de eventos y una centralización de registros de sus actividades (los cuales, de manera complementaria, soportan estrategias de control de integridad), hemos avanzado en la formalización de la confiabilidad de la evidencia digital.

Asimismo, en el desarrollo de *software* o diseño de programas es necesario incluir, desde las primeras fases de la creación de aplicaciones, un momento para la configuración de logs o registros de auditoría del sistema ya que, de no hacerlo, se corre el riesgo de perder *trazabilidad* (3) de las acciones de los usuarios en el sistema y, por tanto, crear un terreno fértil para la ocurrencia de acciones no autorizadas, es decir, se sugiere que la confiabilidad de la evidencia en una arquitectura de cómputo estará en función de la manera como se sincronice la inscripción de las acciones de los usuarios y de un registro centralizado e íntegro de los mismos. Esto reitera la necesidad de un control de integridad de los registros del sistema para mantener su autenticidad.

2.1.4.3 Completitud o Suficiencia

Es la presencia de toda la evidencia necesaria para adelantar el caso; esta característica, al igual que las anteriores, es factor crítico de éxito en las investigaciones en procesos judiciales. Con frecuencia, la falta de pruebas o insuficiencia de elementos probatorios ocasiona la dilación o terminación de procesos que podrían haberse resuelto. En este sentido, los abogados reconocen que, mientras mayores fuentes de análisis y pruebas se tengan, habrá más posibilidades de avanzar en la defensa o acusación en un proceso judicial.

Desarrollar estas particularidades en arquitecturas de cómputo requiere afianzar y manejar destrezas de correlación de eventos en registros de auditoría, es decir, si se cuenta con una arquitectura con mecanismos de integridad, sincronización y centrali-

(3) Trazabilidad - Capacidad de seguimiento y reconstrucción de acciones efectuadas por los usuarios en un sistema

zación, es posible establecer patrones de análisis que muestren la imagen completa de la situación bajo revisión.

La correlación de hechos (definida como el establecimiento de relaciones coherentes y consistentes entre diferentes fuentes de datos para establecer y conocer eventos ocurridos en una arquitectura o proceso) sugiere una manera de probar y verificar la suficiencia de los datos entregados en un juicio.

Si analizamos esta posibilidad, es viable establecer relaciones entre los datos y los sucesos presentados, canalizando las inquietudes y afirmaciones de las partes sobre comportamientos y acciones de los involucrados, sustentando dichas conexiones con acontecimientos o registros que previamente han sido asegurados y sincronizados.

Con esto en mente, la correlación se convierte en factor aglutinante de las características anteriores referenciadas para integridad y confiabilidad de la evidencia, lo que propone un panorama básico requerido en las arquitecturas de cómputo para validar las condiciones solicitadas por la ley en relación con las pruebas.

Es decir, que la correlación de sucesos (como una función entre la centralización del registro de eventos y el debido control de integridad de los mismos) se soporta en una sincronización formal de tiempo y eventos que deben estar disponibles por la arquitectura de cómputo para asegurar la suficiencia del análisis de la información presente en una arquitectura de cómputo.

2.1.4.4. Conformidad con las leyes y reglas de la administración de justicia

Hace referencia a los procedimientos internacionalmente aceptados para recolección, aseguramiento, análisis y reporte de la evidencia digital. Si bien están previstos en el código de procedimiento penal las actividades mínimas requeridas para aportar evidencia a los procesos, existen en medios digitales iniciativas internacionales donde se establecen lineamientos de acción y parámetros que cobijan el tratamiento de la evidencia en medios electrónicos, los cuales deben ser

revisados y analizados en cada uno de los contextos nacionales para su posible incorporación.

2.1.5 Procedimiento forense para el manejo de investigaciones [Torres et al., 2006]

Éste procedimiento forense para el manejo de investigaciones, fue elaborado en el contexto colombiano:

Planeación

Se debe detectar el incidente, el investigador debe familiarizarse con éste y con el entorno en el que ocurrió y determinar el proceso para la recolección de evidencia. Identificar el problema aparente e indagar qué tanto contacto tuvieron los usuarios con el sistema involucrado en el incidente. Para ello se sugiere el desarrollo de entrevistas al personal de la organización que tenga algún tipo de relación con el entorno informático.

Quienes llevamos algunos años en la universidad, sabemos que un cambio de plan de estudios -muy conveniente y necesario plantearlo al menos cada 10 años- conlleva varios años de duras batallas y, lo que es peor, muchas veces influyen además aspectos colaterales de tipo político en el sentido más amplio de la palabra, y la respuesta a lo que demanda el mercado y el sentido común universitario llega tarde y mas a quienes esperan de nosotros una formación de alto nivel, esto es la sociedad a través de nuestros alumnos. Como botón de muestra, basta leer algunos documentos sobre las nuevas tendencias en educación superior en Europa cuyo afán está en homogeneizar estos estudios y cómo han reaccionado de forma distinta los países, sus universidades, las facultades dentro de una misma universidad, etc., cado uno intentando mantener su status quo.

El investigador debe describir con detalle la escena. Registrar información gráfica del lugar ya que también pueden convertirse en evidencia digital: Serán documentos

todas aquellas formas de expresión producto del desarrollo de las técnicas de la comunicación y la informática, incluyendo, por ejemplo: videos y fotografías.

Recolección

Es la etapa más crítica pues se debe recoger la información relevante y conservarla garantizando los requisitos de admisibilidad fijados por la Ley 527 de la Legislación Colombiana: Para valorar la fuerza probatoria de la información digital "habrá de tenerse en cuenta la confiabilidad en la forma en la que se haya generado, archivado o comunicado la información".

Como muchas veces no es posible presentar los sistemas involucrados en una audiencia o tenerlos durante la investigación, se recomienda tomar una copia idéntica de su contenido.

El segundo enfoque toma medidas pasivas que, aunque no corrigen los problemas inmediatamente, permiten analizar el estado del sistema. Además, este esquema permite utilizar otras herramientas, tales como sniffers y honeypots, para recolectar nuevas pruebas que permitan o bien identificar al autor del delito o tener más evidencia.

La cantidad de información que se debe recolectar deber ser decidida por el investigador durante la etapa de planeación, teniendo en cuenta las hipótesis planteadas, las evidencias registradas y los elementos recolectados en los testimonios de los involucrados.

Preservación y aseguramiento de la evidencia digital

En esta etapa se busca garantizar uno más de los requisitos de admisibilidad fijados por la Ley 527 de la Legislación Colombiana: Para valorar la fuerza probatoria de la información digital "habrá de tenerse en cuenta la confiabilidad en la forma en la que se haya conservado la integridad de la información y la forma en la que se identifique a su iniciador".

Durante el proceso de recolección y de análisis de la evidencia digital, es deber del investigador utilizar algún método para mantener y verificar su integridad, ya que un punto clave en la preservación de evidencia digital es que se recolecte sin alterarla y evitar su manipulación futura. En Colombia se cuenta con las entidades de certificación quienes expiden certificados de firma digital que pueden ser útiles para estos procesos.

En la ley 527 de 1999 "Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:
Es única a la persona que la usa.
Es susceptible de ser verificada.
Está bajo el control exclusivo de la persona que la usa.
Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

El análisis de la evidencia digital

Es utópico pretender que el investigador sea experto en todas las áreas necesarias para el análisis de la evidencia. Por el contrario, el valor del investigador se fundamenta en su conocimiento y percepción del entorno tecnológico actual, incluyendo su funcionamiento, sus límites y sus áreas vulnerables. A partir de este conocimiento, debe apoyarse en especialistas que lo asistan en las labores técnicas específicas.

La tarea de recuperación y reconstrucción de la evidencia digital, requiere que se busque eficientemente sobre el contenido de diferentes medios de almacenamiento, con el fin de identificar evidencia relevante. Además, el investigador siempre debe

suponer que puede existir información no visible dentro del medio, pero teniendo en cuenta que este no es siempre el caso y que es parte de su labor determinar la realidad en cuanto a este aspecto.

Un gran obstáculo que se puede presentar durante la investigación, es encontrarse con información cifrada, ya que en muchos casos sólo será posible tener acceso a ella si se dispone de la contraseña o llave que permite visualizarla. Una vez se ha recuperado o se ha encontrado información que podría ser relevante, es necesario realizar un proceso de filtrado que permita extraer la información directamente relacionada con el incidente.

Se debe realizar un procedimiento de limpieza que por un lado conserve la integridad de la información recolectada y que por otro represente en su totalidad el escenario analizado. Por ejemplo, un sistema de logs puede registrar miles de eventos, de los cuales, de acuerdo con la evidencia obtenida, es necesario extraer solamente los relacionados con un equipo en particular.

Una vez se han descartado los datos que no tienen ninguna relevancia con la investigación, se debe iniciar el proceso de clasificación, comparación e individualización de la evidencia. "La clasificación de la evidencia digital, es el proceso por el cual se buscan características que pueden ser utilizadas para describirla en términos generales y distinguirla de especimenes similares".

La clasificación de la evidencia digital es útil al reconstruir un delito porque puede proveer detalles adicionales, es decir, cuando se combinan estos detalles pueden guiar al investigador hacia evidencia adicional, e inclusive hacia el mismo sospechoso del hecho en cuestión. La evidencia digital puede ser clasificada, comparada e individualizada de diferentes maneras, las cuales deben ser utilizadas a criterio del investigador basado en la evidencia que se haya recolectado hasta el momento.

Para finalizar, es necesario reconstruir el escenario en el que ocurrieron los hechos a partir de la correlación de los diferentes elementos recolectados como evidencia. Es importante tener en cuenta, en lo posible, información diferente de la evidencia digital al reconstruir la escena.

Presentación de la Evidencia Digital

Hasta este punto se ha tratado a la evidencia digital en su forma electrónica, sin embargo, es necesario convertirla en algo que pueda ser revisado e interpretado en una corte. Pero, ¿cómo se puede garantizar la neutralidad de este tipo de presentación?, a pesar de que no existe una respuesta única a esta pregunta, debido a las enormes diferencias que existen entre cada incidente, Sommers, en el documento "Downloads, Logs and Captures: Evidence from Cyberspace", especifica que en la mayoría de los casos puede ser apropiado ofrecer 2 posibilidades. Una "de bajo nivel" en la que se muestre la información tal como es sin ningún tipo de anotación y modificación. Y otra "editada", en la que se encuentre solo la información relevante y que explique que se hizo con ella y por qué. Con este enfoque, es posible realizar una inspección cruzada en la que la copia de bajo nivel es la encargada de sustentar técnicamente los argumentos presentados en la parte editada y comentada.

Además es recomendable clasificar la evidencia para su presentación ante una corte, identificando si los datos:

Verifican los datos y teorías existentes (Evidencia que inculpa).
Contradicen los datos y teorías existentes (Evidencia que exculpa).
Muestran signos de manipulaciones para esconder otros datos.

Actualmente la legislación colombiana, no ofrece pautas generales en los códigos de procedimientos sobre cómo debe ser presentada la evidencia recolectada de un sistema de cómputo, lo cual es una de las razones que dificultan condenar las conductas relacionadas con incidentes informáticos y/o relacionados con la

informática, adicionalmente, el desconocimiento de los aspectos técnicos básicos y del lenguaje utilizado en este tipo de casos por parte de los funcionarios judiciales, dificulta aún mas la penalización de estos hechos.

2.1.6 Método Científico

Este método científico se suele utilizar para mejorar o precisar teorías previas en función de nuevos conocimientos, donde la complejidad del modelo no permite formulaciones lógicas. Por lo tanto, tiene un carácter predominantemente intuitivo y necesita, no sólo para ser rechazado sino también para imponer su validez, la contrastación de sus conclusiones.

Se podría proponer, para estas tres variantes del método científico, la denominación de método deductivo, método intuitivo y método experimental o método de contrastación, o cualquier conjunto de palabras que hagan referencia a sus diferencias fundamentales y no planteen problemas a la memoria lingüística. En esta misma línea se encuentra la denominación de método lógico deductivo que a veces recibe el método deductivo.

La primera característica del método científico es su naturaleza convencional, la de servir de marco de generación del conocimiento objetivo. Por ello existen múltiples características en función de la perspectiva con que se clasifiquen, se estudien e incluso se denominen.

Una característica de ambos métodos es que pueden ir de lo general a lo particular o viceversa, en un sentido o en el inverso. Ambos utilizan la lógica y llegan a una conclusión. En última instancia, siempre tienen elementos filosóficos subyacentes.

Ambos suelen ser susceptibles de contrastación empírica. Aunque el método deductivo es más propio de las ciencias formales y el inductivo de las ciencias empíricas, nada impide la aplicación indistinta de un método científico u otro a una teoría concreta.

La diferencia fundamental entre el método deductivo y el método inductivo es que el primero aspira a demostrar, mediante la lógica pura, la conclusión en su totalidad a partir de unas premisas, de manera que se garantiza la veracidad de las conclusiones, si no se invalida la lógica aplicada. Se trata del modelo axiomático propuesto por Aristóteles como el método científico ideal.

Por el contrario, el método inductivo crea leyes a partir de la observación de los hechos, mediante la generalización del comportamiento observado; en realidad, lo que realiza es una especie de generalización, sin que por medio de la lógica pueda conseguir una demostración de las citadas leyes o conjunto de conclusiones.

Dichas conclusiones podrían ser falsas y, al mismo tiempo, la aplicación parcial efectuada de la lógica podría mantener su validez; por eso, el método inductivo necesita una condición adicional, su aplicación se considera válida mientras no se encuentre ningún caso que no cumpla el modelo propuesto.

El método hipotético-deductivo o de contrastación de hipótesis no plantea, en principio, problema alguno, puesto que su validez depende de los resultados de la propia contrastación.

La Teoría General de la Evolución Condicionada de la Vida sería, en principio, una teoría basada en el método hipotético-deductivo o método de contrastación de hipótesis.

La teoría de Darwin, por el contrario, estaría encuadrada en el método inductivo; pero que a pesar de encontrar ejemplos contrarios no se invalida sino que se adecua para cuadrar cualquier triángulo.

2.1.6.1 Método Lógico Deductivo

Cuando el hombre tiene unificación de las ideas se tiene el concepto de veracidad. Los filósofos griegos hicieron la primera contribución de importancia al desarrollo de un método sistemático para descubrir la verdad. Aristóteles y sus discípulos

implantaron el razonamiento deductivo como un proceso del pensamiento en el que de afirmaciones generales se llega a afirmaciones específicas aplicando las reglas de la lógica.

El método deductivo aspira a demostrar, mediante la lógica pura, la conclusión en su totalidad a partir de unas premisas, de manera que se garantiza la veracidad de las conclusiones, si no se invalida la lógica aplicada.

Si las premisas del razonamiento deductivo son verdaderas la conclusión también lo será. Este razonamiento permite organizar las premisas en silogismo que proporcionan la prueba decisiva para la validez de una conclusión. Es necesario empezar con premisas verdaderas para llegar a conclusiones válidas.

El razonamiento deductivo utiliza el método deductivo que relaciona tres momentos de la deducción : 1) Axiomatización (1er. principio) se parte de axiomas; verdades que no requieren de demostración 2) Postulación se refiere a los postulados, doctrinas asimiladas o creadas y 3) Demostración, referido al acto científico propio de los matemáticos, lógicos, filósofos, etc. [Dávila, 2006]

2.1.6.1.1 **Razonamiento Deductivo Válido** [Rojo, 1996]

Llamamos razonamiento a un par ordenado $(\{P_i\}: q)$, siendo $\{P_i\}$ un conjunto finito de proposiciones, llamadas premisas, y q una proposición llamada conclusión, respecto de la cual se afirma que deriva de las premisas.

Un razonamiento es deductivo si y sólo si las premisas son evidencias de la verdad de la conclusión, es decir, si $P_1, P_2, P_3, \ldots P_n$ son verdaderas entonces q verdadera. Un razonamiento deductivo es válido si no es posible que las premisas sean verdaderas y la conclusión falsa. De un razonamiento no se dice que es verdadero o falso, sino que es válido o no.

Llamamos regla de inferencia, a todo esquema válido de razonamiento, independientemente de la V o F de las proposiciones componentes. De éste modo toda regla de inferencia es tautológica.

Un razonamiento deductivo es válido cuando el condicional cuyo antecedente es la conjunción de las premisas, y el consecuente es la conclusión, es tautológico.

Son ejemplos de reglas de inferencia:

a) Ley del Modus Ponens:

SI p y $p \rightarrow q$, ENTONCES q

La notación clásica es

$$\begin{array}{l} p \\ p \rightarrow q \\ \hline q \end{array}$$

b) Ley del Modus Tolens:

$$\begin{array}{l} p \rightarrow q \\ \sim q \\ \hline \sim p \end{array}$$

Este esquema es la notación clásica del condicional

$[(p \rightarrow q) \wedge \sim q] \rightarrow \sim p$

c) Ley del silogismo hipotético:

$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline p \rightarrow r \end{array}$$

Es decir, la proposición $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$ es una tautología.

En cambio, el condicional [(p→q) ^ q] → p no es una forma validada de razonamiento, ya que la correspondiente tabla de valores de verdad nos muestra que no es tautológico.

2.1.6.2 Método Inductivo

El método inductivo se conoce como experimental y sus pasos son:
1) Observación, 2) Formulación de hipótesis, 3) Verificación, 4) Tesis, 5) Ley y 6) Teoría. La teoría de la falseación funciona con funciona con el método inductivo, por lo que las conclusiones inductivas sólo pueden ser absolutas cuando el grupo a que se refieran sea pequeño: por ejemplo si uno advierte que los alumnos de pelo rizado de un grupo escolar lograron en ortografía calificaciones superiores a las del promedio, una conclusión legitima será que todos los morenos de ese grupo muestran calificaciones superiores a las del promedio. Pero no es legítimo extraer conclusiones acerca de las calificaciones de los pelirrojos en otros grupos ni en grupos futuros [Dávila, 2006].

El método inductivo crea leyes a partir de la observación de los hechos, mediante la generalización del comportamiento observado; en realidad, lo que realiza es una especie de generalización, sin que por medio de la lógica pueda conseguir una demostración de las citadas leyes o conjunto de conclusiones.

Dichas conclusiones podrían ser falsas y, al mismo tiempo, la aplicación parcial efectuada de la lógica podría mantener su validez; por eso, el método inductivo necesita una condición adicional, su aplicación se considera válida mientras no se encuentre ningún caso que no cumpla el modelo propuesto.

CAPÍTULO 3
MARCO APLICATIVO

CAPITULO 3
MARCO APLICATIVO

3.1 Axiomatización

La evidencia digital es muy frágil y puede perderse o modificarse con demasiada facilidad, un mal manejo de la misma produce una disminución de la credibilidad que se tenía sobre ésta y una posible impunidad, al ser anuladas o inadmisibles en un juicio.

Esa evidencia digital será utilizada para descubrir o formar los elementos del delito o descubrir la identidad del sujeto activo, y luego, en su caso aportar la misma al proceso penal a fin de poder obtener la condena del mismo, sin sufrir las consecuencias de la nulidad de las pruebas o la inadmisibilidad de éstas en el juicio.

Para que la evidencia digital sea admisible en un proceso jurídico en nuestro país, los procedimientos informático forense deben garantizar que:

- ✓ La evidencia digital sea auténtica
- ✓ La evidencia digital sea confiable
- ✓ La evidencia digital sea suficiente
- ✓ La evidencia digital se encuentre en conformidad con las leyes y reglas de la administración de justicia.

3.2 Postulación

Es imprescindible que de suscitarse un delito informático, antes de empezar a poner en práctica éste método informático forense previamente se debe contar con una orden judicial o requerimiento de un fiscal, se debe considerar que los pasos de los procedimientos que permitan manejar la evidencia digital deben estar respaldados en el marco legal, es decir que no se debe violar las leyes.

3.2.1 PROCEDIMIENTO PARA IDENTIFICAR LA EVIDENCIA DIGITAL A SECUESTRAR (4)

Para no alterar o perder ninguna de las evidencias, ya sean estas digitales o físicas en el lugar de los hechos, a fin de poder relacionar las mismas entre si o en su caso poder hacerlo con el probable responsable, es imprescindible identificar en primer lugar las evidencias que servirán en la investigación del posible ilícito, para tal efecto tomar en cuenta los pasos que se detallan a continuación:

1) Asegurar el acceso y control de los suministros de luz, ya que algunos equipos al ser apagados de manera incorrecta pueden dañarse (lo que haría irrecuperable la información).

2) Si al momento de ingresar al lugar alguien se encuentra operando en el equipo o sistema involucrado en el posible ilícito, tomar nota de la situación y fotografiarlo cuando aún está sentado en posición de operador.

3) Pedir a la persona que se encuentra en el equipo que suspenda de manera inmediata lo que está haciendo y tratar de tener control de las actividades que realiza hasta que se encuentre separado del equipo y los periféricos.

4) Una vez que se encuentra garantizado el cierre del área, proceder a tomar fotografías del estado y posición de los equipos, como así mismo de sus puertos (conectores de cables, lectores de CDs, lectores de disquets), es decir registrar en medio fotográfico o video la escena del hecho, detallando los elementos informáticos allí involucrados.

---

(4) Secuestrar.- En informatica forense éste termino indica que se debe sustraer evidencia del lugar donde aconteció el delito informático Embargo de una cosa o de un bien por orden judicial

5) Fotografiar una toma completa del lugar donde se encuentren los equipos informáticos y de ser posible realizar filmaciones del lugar del hecho.

6) Fotografiar la existencia de cámaras de video o de fotografía, instaladas en la escena de los hechos para poder tener plena certeza de la posibilidad de la obtención de pruebas adicionales de la relación usuario-equipo.

7) Tener extrema precaución de no tropezar, jalar o cortar cables que pudieran representar conexiones de equipos, periféricos o conexiones de entrada o salida de datos.

8) Identificar los dispositivos informáticos que almacenen grandes volúmenes de información digital (computadora de escritorio, computadora portátil y discos duros portátiles).



9) Identificar memorias USBs, DVDs, CDs, disquets relevantes a la investigación, puesto que puede encontrarse cantidades importantes de los mismos.

10) Observar e identificar si en la escena del hecho existe más de un equipo que se encuentra involucrado en el posible ilícito.

11) Identificar si existen equipos que estén conectados a una línea telefónica, y en su caso el número telefónico para registrarlo en el acta de allanamiento para el caso de delitos informáticos como observaciones (ver Figura 3, pág.37).

12) Identificar si el equipo tiene tarjeta de red inalámbrica, si existe fotografiarla.

13) Identificar si existen periféricos conectados a los equipos informáticos, realizar fotografías de las mismas.

14) Identificar el posible delito que se hubiese cometido en la escena del hecho, determinar los presuntos actores involucrados, máquinas y/o usuarios y la posible participación que tuvo cada uno.

15) Realizar entrevistas al personal de la organización que tenga algún tipo de relación con el entorno informático, con la finalidad de poder determinar: Qué tipo de sistemas informáticos se usan, qué tipo de registros generan, si se cuenta con políticas de seguridad o no y quiénes son responsables del funcionamiento de los equipos y los servicios de la organización.

16) Separar las personas que trabajen sobre los equipos informáticos lo antes posible y no permitirles volver a utilizarlos, por que estuviesen contaminando la escena del hecho. Si es una empresa, se debe identificar al personal informático interno (administradores de sistemas, programadores) o a los usuarios de aplicaciones específicas que deban posiblemente someterse a la investigación.

17) Identificar el nombre del dueño o usuarios del equipamiento informático ya que luego pueden ser de utilidad para la investigación. Siempre que sea posible obtener contraseñas de aplicaciones, dejarlas registradas en el acta de allanamiento de acuerdo al formato de ésta.

18) Observar detalladamente la escena del hecho y levantar un mapa de los elementos informáticos involucrados, el cual se deberá adicionar al acta de allanamiento de la escena del hecho, si fuese posible identificar además nombres de usuarios y roles; en caso de existir varios equipos enumérelos en el mapa, dicha numeración de los equipos la utilizará en el procedimiento de adquisición de la evidencia digital.

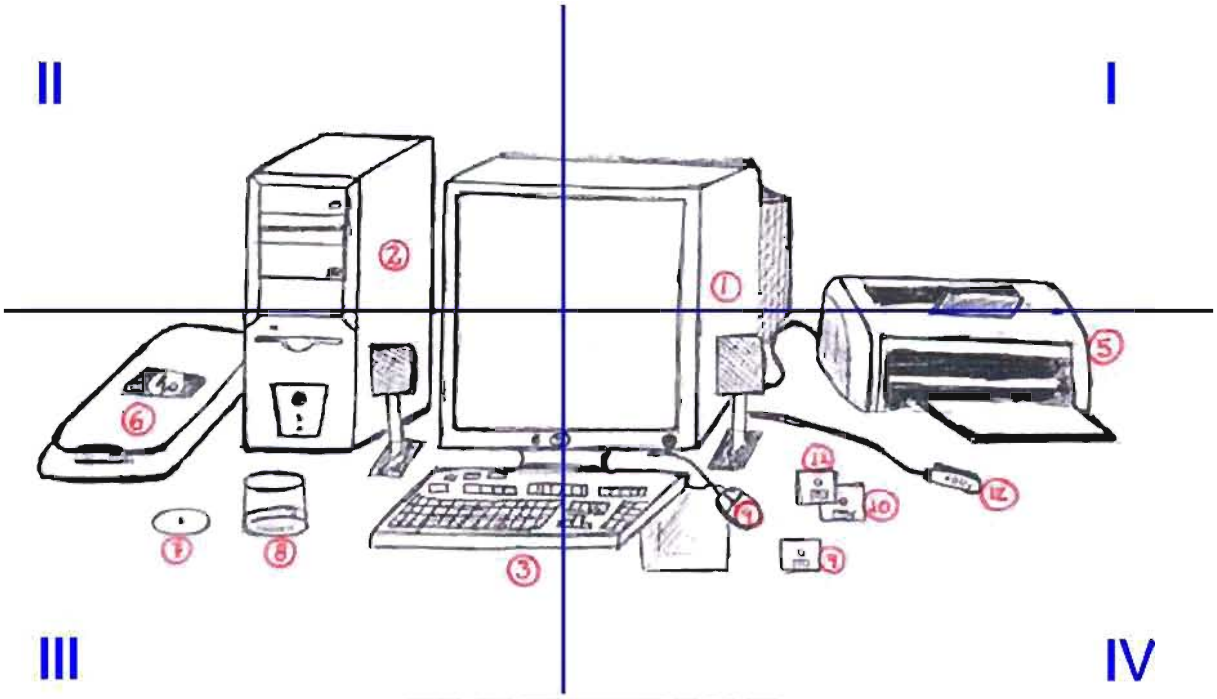


Figura 2. Mapa de los elementos informáticos involucrados

Fuente: Elaboración Propia

Elaborar un pequeño mapa a mano alzada, indicando las posiciones exactas donde se encontraban los elementos informáticos involucrados, para tal situación se puede utilizar el siguiente planteamiento, que propongo:

- Enumerar cada elemento informatico involucrado y plasmarlo según sus posiciones en un plano de cuadrantes, donde se podrá ubicar cada dispositivo en un cuadrante específico, tomando el monitor de la computadora involucrada como centro de referencia, esto con la finalidad de reconstruir con exactitud la ubicación física de cada objeto.

- En el caso que varias computadoras estén involucradas, hacer para cada computadora un mapa, pero describir claramente, el lugar de la escena del hecho al cual corresponde esa computadora.

19) Clasificar la información de la organización, de tal forma que se pueda establecer cuál es la evidencia más relevante y formal que se tiene. Para ello, las oficinas de archivo o documentación en conjunto con el área de tecnología deben adelantar un estudio de las características de la información que soporta decisiones administrativas y sus medidas tecnológicas de protección, almacenamiento y recuperación posterior.

20) Identificar además las evidencias necesarias, electrónicas o no de la existencia de los vínculos entre el sujeto y el equipo, para lo cual se recomienda buscar, además de los bienes en sí mismos, los siguientes comprobantes de posible existencia:

- ✓ Comprobantes de pago y/o facturas de servicio de Internet, conexión satelital (teléfono y/o internet), facturas de luz, servicio de teléfono, servicio de telefonía celular, servicio de agua, tarjetas de crédito.
- ✓ Anotaciones de claves de usuario o de correos que pudieran encontrarse en soportes distintos a los electrónicos (papeles)
- ✓ Comprobantes de operaciones realizadas con tarjetas de crédito o débito.
- ✓ Comprobantes emitidos por cajeros automáticos.
- ✓ Listados de estados de cuentas bancarias.
- ✓ Plásticos o tarjetas de crédito o débito.
- ✓ Plásticos de tarjetas de hoteles u otras con banda magnética.
- ✓ Facturas de pago de cualquier comercio o institución que puedan relacionarse con la persona o con los números de tarjetas que utiliza o, en su caso con las cuentas bancarias, telefónicas o de internet que se investigan.

Figura 3

Propuesta I:

ACTA DE ALLANAMIENTO PARA
EL CASO DE DELITOS INFORMATICOS

ORGANISMO	CASO N°
DIVISIÓN:	
SEGUIDO POR:	EN CONTRA DE:
DELITO(S):	

En…….. a hrs……..del día……del mes……..…de……años,
ejecución de Mandamiento de Allanamiento ☐ Registro ☐ Secuestro☐ Incautación☐,
expedido por el Juez……
se procedió al acto de Allanamiento en el inmueble ubicado en la Av.Calle/ ……..……..……
……..N° …….. de la Zona……
en presencia de:……..
a quien se puso en conocimiento de la resolución que dispone éste acto procesal y se le entregó una copia del mandamiento.
Por ausencia del habitante en el inmueble, se fijó copia del mandamiento en el la puerta del domicilio allanado.
Acto realizado por el Fiscal……..
Con la intervención de los Investigadores: ……
……y
Los Peritos Informatico Forenses:……
……..
En presencia del testigo:……..
Con CI ☐ RUN ☐ PASAPORTE☐ N°……

Fuente: Elaboración Propia

I. DESCRIPCION DEL LUGAR, COSAS, RASTROS Y EFECTOS MATERIALES, CONSECUENCIA DEL DELITO INFORMATICO

En el desarrollo del actuado se realizaron las siguientes actividades:

II. DESCRIPCION DE LOS ELEMENTOS INFORMATICOS INVOLUCRADOS (e.i.i.) Y SECUESTRADOS

Objeto	Código o Nro. Serie	Características	N° del Mapa de los (e.i.i.)	Cuadrante en el que se encontraba
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				

Fuente: Elaboración Propia

Los objetos secuestrados, debidamente asegurados y sellados quedan en poder de:……..
……
……..……, las copias realizadas de la evidencia digital intangible, debidamente asegurados y sellados quedan en poder de:……....
……

Observaciones:

Con lo que termino el acto a horas…….....del día……del mes……año……firmando al pie los intervinientes:

Fiscal:……..……

Investigador Asignado al caso:…… ……

Investigador Especial:…… ……..

Perito Informático Forense (1):…… ……

Perito Informático Forense (2):…… ……

Propietario:…… ……

Ocupante:……... ……

Testigo:……... ……

Otros:……..... ……

Fuente: Elaboración Propia

3.2.2 PROCEDIMIENTO PARA ADQUIRIR LA EVIDENCIA DIGITAL

Consideraciones previas

No se espera que toda la información que se adquiera deba ser admisible como evidencia, pues mucha de esta información será utilizada para, a través de ella, descubrir evidencia admisible.

Antes de empezar a adquirir las evidencias digitales en una escena del hecho y cuando se esté llevando a cabo tal cometido, tomar en cuenta las siguientes consideraciones:

- ✓ Utilizar pulseras antiestáticas para evitar daños en los componentes electrónicos y guantes de látex para no alterar, encubrir o hacer desaparecer las huellas dactilares existentes en el equipo.


- ✓ Tener los elementos necesarios: bolsas antiestáticas, sobres antihumedad, cajas de cartón (preferiblemente utilizar el material de embalaje que fue dispuesto por el fabricante de los dispositivos electrónicos que serán secuestrados) y otros materiales que crea necesario; no utilizar documentos o material de la misma escena del hecho como empaque.



- ✓ Proceder con el acordonamiento del lugar y asegurar el área dónde ocurrió el incidente, con el fin de custodiar la escena del hecho y así fortalecer la cadena de custodia (ver Anexo E) y adquisición de la evidencia.

- ✓ Registrar todo lo que se va adquiriendo como evidencia, en el formulario de adquisición de evidencia digital (ver Figura 5, pág.51).

- ✓ Según el RFC 3227 (5), la evidencia debe ser recolectada de lo más a lo menos volátil. A continuación se presenta una posible clasificación según el orden de volatilidad:

  - **Evidencia altamente volátil**

  CPU (Registros, Caché), Memoria de Video. Usualmente la informacion en estos dispositivos es de mínima utilidad, pero debe ser capturada como parte de la imagen de la memoria del sistema.

  - **Evidencia medianamente volátil**

  La memoria RAM, incluye información sobre los procesos en ejecución, el hecho de capturarla hace que cambie. Requiere conocimiento especializado para poder reconstruirla, pero no se requiere mucho conocimiento para hacer una búsqueda de palabras clave.

  Tablas del Kernel (Procesos en ejecución), permiten analizar los procesos que pueden ser evidencia de actividades no autorizadas.

  - **Evidencia poco volátil**

  Medios Fijos (Discos Duros), Incluye área de swap, colas, directorios temporales, directorios de registros. La información recolectada en el área de swap y las colas permite analizar los procesos y la información de los mismos en un punto del tiempo en particular. Los directorios permiten reconstruir eventos.

---

(5) RFC 3227 (Request For Comment) Petición de comentarios Documento que describe el orden de volatilidad de la evidencia digital

Medio Removible (disquets, memorias USBs, CDs, DVDs), usualmente son dispositivos para almacenamiento de contenidos históricos del sistema. Si existen previamente a un incidente pueden ser usadas para acotar el periodo de tiempo en el cual sucedió.

Medio Impreso (papel), difíciles de analizar cuando hay muchos, ya que no se pueden realizar búsquedas automáticas sobre ellos.

- ✓ Registrar todas las actividades que se estén efectuando al momento de proceder con la recolección, de tal manera que se pueda auditar el proceso en sí mismo y se cuente con la evidencia de este proceso.

- ✓ Las evidencias que se recolecten de la escena del hecho, se transportan hasta los ambientes predefinidos puede ser la oficina de auditoria interna, los laboratorios del Instituto de Investigación Forense, ambientes de la Fiscalia, o de ser necesario se puede proceder al anticipo de prueba (ver apartado 3.2.5), se transportan siempre apuntando la lista, en el cuaderno de investigaciones, bajo constancia en acta, con la firma de todos los participantes y un testigo de actuación (6).

(6) **NUEVO CODIGO DE PROCEDIMIENTO PENAL – BOLIVIA: Artículo 121º.- (Testigos De Actuación).**
Podrá ser testigo de actuación cualquier persona con excepción de los menores de catorce años, los enfermos mentales y los que se encuentren bajo el efecto de bebidas alcohólicas o estupefacientes

3.2.2.1 Procedimiento para adquirir la evidencia digital: Si los equipos pueden ser retirados de la escena del hecho

1) Levantar de manera individual todos los medios de soporte que se encuentren separados del equipo (CDs, DVDs, disquets, memorias USB) bajo un respectivo listado almacenarlos en conjunto en un sobre antiestático y verificar si los equipos se encuentran apagados o encendidos, asentar en el acta su estado.



2) Si en la escena del hecho existe más de un equipo, identificar claramente cada uno de ellos por medio de números (mismos números que colocó en el mapa de los elementos informáticos involucrados realizado en el procedimiento de identificación de la evidencia a secuestrar) con etiquetas firmadas y en cada pieza que se retire de cada uno de ellos colocar el número que se asignó al equipo. Además identificar en las fotografías el número que se asigna a cada equipo.

3) En caso de encontrarse encendido el equipo, no apagar pues se podría perder información volátil (el contenido de la memoria, procesos que se están ejecutando, usuarios que están dentro del sistema, archivos que están abiertos), realizar la verificación de conexiones inalámbricas o de la existencia de puertos de red, que pudieran ser fuente de acceso para modificar los contenidos, para aislar de intrusiones externas.

4) Si en el equipo existiese una tarjeta de red inalámbrica, retirarla y precintar el lugar de donde se retiró, posteriormente dicha tarjeta debe ser fotografiada e introducida en una bolsa para su aseguramiento, además precintar de manera inmediata las conexiones que se retiren. Si la tarjeta fuese interna, localizar la tecla de anulación del servicio inalámbrico y desactivar rápidamente el mismo.

5) Inmediatamente realizar una fotografía detallada de la imagen de la pantalla, si se trata de un protector de pantalla o el monitor estuviese en descanso, con la utilización de guantes de látex mover lentamente el ratón hasta que aparezca la imagen del programa en proceso al momento anterior al inicio del ahorro de energía del equipo.

6) Realizar fotografías inmediatamente, de la imagen de la pantalla que aparece luego de esa operación. Si aparece la pantalla pidiendo la clave fijar la instancia con fotografías, pero no efectuar otro movimiento o tecleo de alguna clave.

7) Añadir en actas la hora en que fueron realizadas las tres operaciones, es decir, la primera fotografía, el movimiento del ratón y la segunda fotografía de la pantalla.

8) Realizar la extracción original de datos de las unidades de

disco y la memoria RAM (clonación de discos y de memoria, es decir realizar una copia bit a bit), para evitar la pérdida de la información volátil o la modificación de datos o registros de entrada al equipo, usando software forense (ver Anexo D), ademas hallar el valor hash respectivo.

El valor hash es una cadena de caracteres y números, obtenida a través de un algoritmo estándar (HASH o función resumen) aprobado internacionalmente los mas utilizados son el MD5 y el SHA-1, a partir de un conjunto de datos, los valores hash generados por dicho algoritmo son únicos.

El valor hash obtenido también debe registrarse en el formulario de adquisición de evidencia digital (ver Figura 5, pág.51), para demostrar la integridad y autenticidad de la evidencia digital original, el cual ayudará a probar que no se ha alterado la evidencia luego de que la computadora llego a su posesión, para negar alegatos de que se ha cambiado la información original.

Por ejemplo, obteniendo los valores hash de los siguientes disquets 1, 2 y 3 donde cada uno almacena información relevante, tenemos:

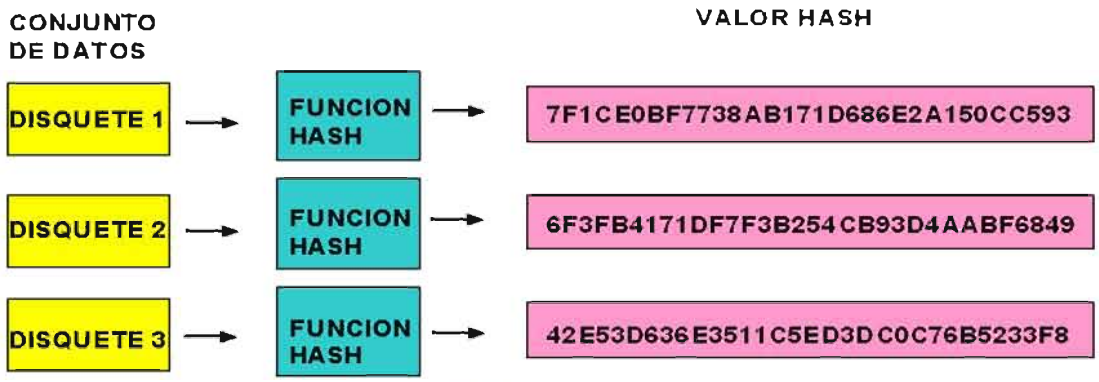


Figura 4. Ejemplo de Valores Hash

Fuente: Elaboración Propia

9) Si el equipo se encuentra apagado no encender, por que se podría contaminar la evidencia, o si se encontraba encendido pero ya se realizó los pasos anteriores apagar el equipo, en ambos casos continuar con los siguientes pasos:

10) Empezar a desconectar y a desmontar un equipo a la vez, para evitar confundir las piezas o cables de cada uno de ellos. Cuando un equipo se encuentre completamente desmontado, retirarlo de la escena del hecho, para poder empezar con el siguiente equipo.

11) Desconectar el cable que conecta el equipo a la energía eléctrica de la pared e inmediatamente realizar el precintado, firmado por la autoridad competente y en su caso los testigos de actuación, sobre el lugar del conector que se retira.

12) Desconectar el otro extremo del mismo cable que se encuentra en la computadora y repetir la operación de precintado y etiquetas firmadas, identificar el cable retirado, por medio de etiquetas firmadas y colocar el mismo en las bolsas de evidencia.

13) Desconectar e identificar el cable de energía eléctrica del monitor con etiqueta, bajo las mismas mecánicas y cuidados del anterior, colocarlo en bolsa de evidencia del mismo modo, además de identificar y desconectar el cable que conecta el monitor con la torre y precintar el lugar del que se retira.

14) Precintar sobre los bordes de apertura del monitor, para evitar que pueda retirarse cualquier pieza del exterior o interior del mismo, sin que ello pudiera ser detectado en revisiones posteriores.

15) Proceder al retiro del teclado (con guantes de látex para evitar alterar las huellas dactilares que pudieran existir en esa área del equipo), precintando luego el sitio donde el mismo estaba conectado y realizar el precintado del extremo del conector del teclado o usar una bolsa de polietileno que se pega al cable.

16) Colocar el teclado en bolsa separada a fin de poder practicar luego las medidas forenses huellas dactilares si ellas se requieren en momentos posteriores del proceso.

17) Proceder de la misma forma que se procedió con el teclado, con el ratón de la computadora, tomando las precauciones de precintado ya descritas.

18) Apagar los periféricos que se encuentren encendidos, previa anotación en el acta respectiva del estado en que se encontraban al inicio del procedimiento, dejando constancia de los números de serie de cada equipo para luego poder diferenciar uno del otro.

19) Desconectar todos los periféricos (impresoras, escáneres, lectores de discos, grabadoras o cualquier otro que se encuentre conectado al equipo), previamente fotografiar el lugar de conexión y posterior precintado en cada caso de los lugares donde se encuentran conectados, dejando constancia de ello en el acta y en el precinto donde además de las firmas, se debe agregar: conexión de <nombre del periférico>, marca, modelo, número de serie, para poder reconstruir la conformación original del equipo, de ser necesario.

20) Al momento de desconectar cada equipo, etiquetarlo, dejando constancia de a que computadora se encontraba conectado, luego de desconectado y etiquetados sus cables de conexión, precintar cualquier punto de entrada o salida de datos (es decir cualquier conector que pudiera tener el equipo) y los accesos de corriente eléctrica.

21) Si se trata de unidades de lectura de tarjetas, de disquets o de CDs, precintar los accesos a la misma. Si se trata de unidades de almacenamiento internas, debe procederse también al precintado de los tornillos de acceso de su exterior, para evitar que pueda ser abierto y puedan retirase, cambiarse o modificarse piezas.

22) Colocar cada periférico en bolsas o cajas individuales e identificadas, para que no exista confusión.

23) Proceder al precintado de la torre, sellando todos los accesos posibles, como puertos USBs, lectores de DVD, CDs, puertos de impresora, teclados, conexiones de red, o cualquier otro que se encuentre luego de una exhaustiva revisión del mismo, posteriormente colocar cada torre en una caja individual, precintada e identificada.

3.2.2.1.1 Si se trata de equipos portátiles

Realizar los pasos 1), 2), 3), 4) y los pasos 5), 6), 7) (ver apartado 3.2.2.1), considerando que se debe pasar suavemente el dedo por el mouse incorporado usando guantes de látex, proseguir con los pasos que a continuación se detallan:

I. Fotografiar al equipo y su número de serie, precintar todos sus mecanismos, conexiones de entrada y salida, proceder a retirar el equipo, al llegar al *ambiente predefinido* (7) volver a conectarlo a la corriente para evitar su apagado al consumirse la batería, si es necesario proceder al anticipo de prueba (ver apartado 3.2.5) amparados en el nuevo código de procedimiento penal.

---

(7) Ambientes predefinidos oficina de auditoria interna, los laboratorios del Instituto de Investigación Forense, ambientes de la Fiscalia u otro dispuesto por la orden del juez o del fiscal

II. Si se encuentra apagado, proceder al precintado y retirar los cables eléctricos, precintado e identificando dicha actividad, dejar constancia en el acta de allanamiento, teniendo el cuidado de no dañar la evidencia digital.

3.2.2.2 Procedimiento para adquirir la evidencia digital: Si los equipos no pueden ser retirados de la escena del hecho

Si por su excesivo tamaño o por otros motivos, los equipos no pudieren ser retirados, se debe asegurar la escena del hecho y se deben tomar en cuenta los siguientes puntos, para realizar la recolección de componentes internos.

Si el equipo se encuentra encendido realizar los pasos 1), 2), 3), 4), 5), 6), 7) y 8) anteriormente descritos al inicio del procedimiento de adquisición de la evidencia digital (ver el apartado 3.2.2.1), si el equipo se encuentra apagado no encender por que se podría contaminar la evidencia o si se encontraba encendido, pero ya se realizó los pasos anteriores, apagar el equipo, en ambos casos continuar con los siguientes pasos:

a) Cuando el equipo se encuentra apagado, pueden desmontarse los medios de almacenamiento que se encuentren en el equipo, desconectar e identificar todos los cables del equipo, proceder a la apertura del mismo por medio de la remoción de su carcaza.

b) Al abrir la carcaza, fotografiar la posición y estado de los medios a extraer, realizar fotografías de aproximación de cada medio y de sus números de serie, asentando los mismos en el formulario de adquisición de la evidencia digital (ver Figura 5, pág.51) de manera referenciada a las fotografías de aproximación y la general.

c) Retirar los medios de almacenamiento, que serán los que se deben asegurar, al remover los cables de conexión del medio, se debe precintar cada uno de ellos con identificación de la posición que ocupaban en el equipo y haciendo lo mismo con los puntos de conexión del equipo.

d) Terminada esa tarea, realizar el precintado debido a todos los tornillos del medio extraído, luego empacar el medio en caja o bolsa por separado, dejando constancia de todo lo realizado en el acta de allanamiento, donde se registran las actividades realizadas (ver Figura 3, pág.37).

e) Culminadas las operaciones, la carcaza debe ser colocada nuevamente, precintar la misma y sus tornillos de extracción para poder preservar el resto del equipo, por si se presentara la necesidad de pruebas posteriores.

Propuesta II:

FORMULARIO DE ADQUISICIÓN DE EVIDENCIA DIGITAL

Caso N°:			Expediente Judicial N° ……..		Form. N°1
Fiscal a cargo:					
Investigador Asignado:					
Perito Informático Forense:					
Tipo de Caso:					
Localización donde se obtuvo la evidencia:					
Articulo	Código	Descripción de la evidencia	Serial	Fabricante	Modelo
Evidencia recuperada por:	Recolección de elem. inf. ☐	Volcado de bits ☐	Extracción de unidades de almacenamiento internas ☐	Recolección del equipo de comp. ☐	Fecha/Hora:
Herramienta Forense utilizada:					
Si realizó volcado de bits:		Valor Hash:			
Evidencia entregada a:			Recibe conforme:……	Entregó conforme:……	Fecha/Hora:
Departamento:		Provincia:	Localidad:		

Figura 5: Formulario de adquisición de evidencia digital
Fuente: Elaboración Propia

3.2.3 PROCEDIMIENTO PARA PRESERVAR LA EVIDENCIA DIGITAL

Para preservar la evidencia digital que fue recolectada en el procedimiento de adquisición, tomar en consideración los pasos que se detallan a continuación:

1) Evitar tocar el material informático sin uso de guantes de látex, ya que dependiendo el objeto de la investigación, el teclado, monitores, mouse, disquets, CDs, DVDs, pueden ser utilizados para análisis de huellas dactilares.

2) Impedir que cualquier persona, realice búsquedas sobre directorios o intente ver la información almacenada ya que se altera y destruye la evidencia digital.

3) No permitir que personal no idóneo manipule la evidencia digital, pues podría dañar, modificar y/o destruir información importante que podría servir para el esclarecimiento de un delito informatico.

4) Realizar un informe y hacer conocer si la evidencia digital ha sido previamente manipulada por personal no idóneo, ya que al realizar el análisis de datos y detectar que la información original ha sido alterada, la evidencia pierde su valor probatorio.

5) En muchos casos no se puede realizar copias de la evidencia original por impedimentos técnicos u otras razones de tiempo y lugar. En estos casos tener mayor cuidado de preservar la evidencia digital, pues de ocurrirse un daño probablemente no se podrá obtener nuevamente la evidencia tal como se encontró en primera instancia.

6) Usar bolsas especiales antiestáticas para almacenar disquets, CDs, DVDs y otros dispositivos de almacenamiento informáticos que sean electromagnéticos (si no se cuenta, pueden utilizarse bolsas de papel madera). Evitar el uso de bolsas plásticas, ya que pueden causar una descarga de electricidad estática que puede destruir los datos.

7) Mantener la cadena de custodia del material informático transportado y llenar el acta para cadena de custodia en el caso de delitos informáticos (ver Figura 6, pág.55), además tener en conocimiento que es responsabilidad del personal policial la alteración de la evidencia antes de que sea objeto de una pericia informática en ambientes predefinidos para la preservación de la misma.

8) Preservar y resguardar el material informático en ambientes donde no deberán exponerse a campos electromagnéticos, ademas donde el acceso a dichos ambientes sea estrictamente controlado. Los elementos informáticos son frágiles y deben manipularse con precaución, por personas idóneas en la manipulación de evidencia digital.

9) El punto clave en la preservación de la evidencia digital es que se recolecte sin alterarla y evitar su manipulación futura, si se contará con entidades de certificación quienes expiden certificados de firma digital que pueden ser útiles para estos procesos, sería un gran respaldo, lamentablemente en la actualidad en nuestro país no contamos con éste tipo de entidades.

10) El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:

- ❖ Es única a la persona que la usa y es susceptible de ser verificada.
- ❖ Está bajo el control exclusivo de la persona que la usa.
- ❖ Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
- ❖ Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

NOTA:

En los siguientes casos, no se podrá asegurar la integridad de la evidencia digital (por lo tanto se pierde la posibilidad de utilizar como medio de prueba): **i)** si el material informático tiene rotos los precintos de seguridad que se le hayan puesto al realizar la recolección de la evidencia **ii)** siempre que no esté descrita en el expediente judicial las actividades realizadas por profesionales calificados al utilizar herramientas forenses.

Se recomienda que las autoridades impulsen a entidades que puedan dedicarse a expedir certificados de firma digital, que apoyen a las labores realizadas por profesionales informatico forenses.

Figura 6: Propuesta III

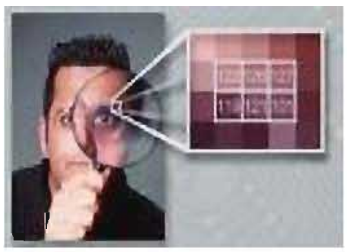
ACTA PARA CADENA DE CUSTODIA EN EL CASO DE DELITOS INFORMÁTICOS

Artículo	Código	Fecha/ Hora	Entregado por:	Recibido por:	Proposito y ubicación
			Nombre: Organización: Firma:	Nombre: Organización: Firma:	
			Nombre: Organización: Firma:	Nombre: Organización: Firma:	
			Nombre: Organización: Firma:	Nombre: Organización: Firma:	
			Nombre: Organización: Firma:	Nombre: Organización: Firma:	
			Nombre: Organización: Firma:	Nombre: Organización: Firma:	
Disposición Final de la evidencia					
Acción Final: Registrar los datos de quienes mantengan la cadena de custodia			Personal receptor de la evidencia digital **Nombre** **Firma** **Fecha y Hora** 1)		
			2)		
			3)		
			4)		

Fuente: Elaboración Propia

3.2.4 PROCEDIMIENTO PARA ANALIZAR LA EVIDENCIA DIGITAL

Realizar el análisis de evidencia digital es una labor muy delicada, por esto es importante prever realizando dos copias de seguridad de los medios originales y trabajar sobre tales copias. Así, si se comete un error que altere la información en una de las copias, se pueda minimizar el impacto en la investigación realizando de nuevo un duplicado a partir de la otra copia y no se perderá la validez e integridad de la evidencia.



La tarea de recuperación y reconstrucción de la evidencia digital, requiere que se busque eficientemente sobre el contenido de diferentes medios de almacenamiento, con el fin de identificar evidencia relevante. Además, siempre se debe suponer que puede existir información no visible dentro del medio, pero teniendo en cuenta que este no es siempre el caso y que es parte de su labor determinar la realidad en cuanto a este aspecto.

Un punto crítico en este tema es la localización de información específica vinculada con una determinada causa. En muchos casos, el análisis de datos requerirá un trabajo interdisciplinario entre el informatico forense y el operador judicial -juez, fiscal- que lleve la causa, a fin de determinar aquellas palabras clave que son de interés para la investigación. Si bien las herramientas forenses permiten realizar análisis de datos mediante palabras clave, y el investigador puede extraer ciertas palabras esenciales para la búsqueda de evidencia, los aportes desde el punto de vista del operador judicial pueden contribuir a obtener mejores resultados.

Los atributos de mayor interés para el informático forense son: el nombre del archivo, fecha y hora de la última modificación, acceso o creación de un archivo, los accesos directos y los de Internet, son algunos de los elementos sobre los que se realiza habitualmente el análisis de datos, para archivos de texto es usual utilizar

herramientas forenses (ver Anexo D) como EnCase para buscar expresiones regulares.

Un gran obstáculo que se puede presentar, es encontrarse con información cifrada, ya que en muchos casos sólo será posible tener acceso a ella si se dispone de la contraseña o llave que permite visualizarla. Una vez se ha recuperado o se ha encontrado información que podría ser relevante, es necesario realizar un proceso de filtrado que permita extraer la información directamente relacionada con el incidente.

Realizar una limpieza de la información que se tiene, que por un lado conserve la integridad de la información recolectada y que por otro represente en su totalidad el escenario analizado.

Una vez se han descartado los datos que no tienen ninguna relevancia con la investigación, se debe iniciar el proceso de clasificación, comparación e individualización de la evidencia. "La clasificación de la evidencia digital, es el proceso por el cual se buscan características que pueden ser utilizadas para describirla en términos generales y distinguirla de especimenes similares". La clasificación de la evidencia digital es útil al reconstruir un delito porque puede proveer detalles adicionales, es decir, cuando se combinan estos detalles pueden guiar hacia evidencias adicionales, e inclusive hacia el mismo sospechoso del hecho en cuestión.

La evidencia digital puede ser clasificada, comparada e individualizada de diferentes maneras, las cuales deben ser utilizadas a criterio del profesional informatico forense, basado en la evidencia que se haya recolectado hasta el momento:

Contenido: Un e-mail, por ejemplo, puede ser clasificado por su contenido como SPAM, y puede ser individualizado a partir del contenido de sus encabezados, información que por lo general no es visible para el usuario. Por ejemplo, por su dirección de origen.

Función: El investigador puede examinar cómo funciona un programa para clasificarlo y algunas veces individualizarlo. Por ejemplo, un programa que inesperadamente transfiere información valiosa desde un computador confiable a una locación remota podría ser clasificado como un caballo de Troya y puede ser individualizado por la localización remota a la que transfiere la información.

Características: los nombres de archivo, extensiones e inclusive los encabezados internos que identifican los diferentes formatos de archivo que existen pueden ser de utilidad en la clasificación de la evidencia digital.

Para finalizar, es necesario reconstruir el escenario en el que ocurrieron los hechos a partir de la correlación de los diferentes elementos recolectados como evidencia. Es importante tener en cuenta, en lo posible, información diferente de la evidencia digital al reconstruir la escena.

A CONSIDERAR:
Se debe tener conocimiento de la herramienta forense que se usa en el análisis, para poder explicar aspectos técnicos, en caso que así lo requiera la autoridad competente, pues el informático forense al ser perito en una determinada investigación, debe estar preparado para dar su testimonio.

La computadora no debe ser operada ni procesada para su análisis hasta que se hayan realizado copias de todos los discos rígidos y disquets. Toda la recuperación forense debe ser realizada en las copias y no en los discos originales. La evidencia original no deberá tocarse a menos que existan circunstancias extremas que así lo demanden.

Posterior al análisis obtener nuevamente el valor hash para comparar con el que se obtuvo en primera instancia, el cual se registró en el formulario de adquisición de la evidencia digital, y así demostrar que se analizó sobre la misma evidencia digital.

3.2.5 PROCEDIMIENTO PARA QUE LA EVIDENCIA DIGITAL SEA PERMITIDA LEGALMENTE

De aplicarse al inicio o en cualquier etapa procedimental pruebas nulas, de dudosa obtención o que afecten garantías constitucionales como la privacidad, el que nadie puede ser obligado a declarar en su propia contra o cualquier otra, de hecho la investigación y el mismo proceso tendrán en su interior el mismo defecto que arrastran desde sus inicios, por lo cual serán nulas o inadmisibles en un juicio, según el Nuevo Código de Procedimiento Penal (NCPP) vigente en Bolivia.

NCPP - BOLIVIA: Artículo 13º.- (Legalidad de la Prueba)

I. *Los elementos de prueba sólo tendrán valor si han sido obtenidos por medios lícitos e incorporados al proceso conforme a las disposiciones de la Constitución Política del Estado y de este Código.*

II. *No tendrá valor la prueba obtenida mediante torturas, malos tratos, coacciones, amenazas, engaños o violación de los derechos fundamentales de las personas, ni la obtenida en virtud de información originada en un procedimiento o medio ilícito.*

NCPP - BOLIVIA: Artículo 71º.- (Ilegalidad de la Prueba).

Los fiscales no podrán utilizar en contra del imputado pruebas obtenidas en violación a la Constitución Política del Estado, Convenciones y Tratados internacionales vigentes y las leyes.

Con la finalidad de que no existan nulidades procedimentales, es necesario que se cuente con una orden judicial o requerimiento de un fiscal, para poder realizar la identificación, adquisición y preservación de la evidencia digital puesto que al no compartir las características de los demás bienes, no se puede tomar una orden de cateo

genérico como suficiente, púes con éste no podremos realizar ningún tipo de inspección a los sistemas electrónicos o en otro caso asegurarlos.

La apertura de un equipo informático o bien su aseguramiento implica la posibilidad de violentar garantías constitucionales, lo que, en definitiva debe ser siempre ordenado y controlado por un juez competente.

El Ministerio Público (8) debe solicitar de manera expresa el aseguramiento de los medios y equipos electrónicos que pudieran contener información.

Con las respectivas previsiones, la evidencia contenida en los equipos o en los medios asegurados puede ser incorporada correctamente al expediente (averiguación previa o proceso judicial) sin objeciones sobre la legalidad de su obtención, pues se estuviese respetando de manera plena las garantías constitucionales involucradas en el proceso.

El Ministerio Público debe incluir en su solicitud expresa la recolección de información y/o el vaciado de datos (copia bit a bit), ya que se puede dar el caso de que el aseguramiento sea físicamente imposible, pues varios equipos no pueden ser movidos en relación directa con su tamaño o bien con el hecho de que de ser retirados podría perderse información de los registros que se están procesando al momento del operativo.

El profesional informático forense en una investigación de delitos informáticos llega a ser un perito de ésta disciplina, quien en algunos casos trabajará en una misma escena del hecho con otros peritos, por lo cual es indispensable tomar previsión de solicitar al juez o al fiscal según sea el caso, la facultad de fotografiar y filmar, realizar

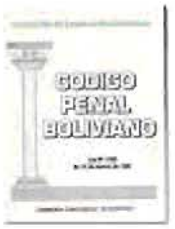
---

(8) **Ministerio Público** - Órgano constitucional que tiene por finalidad promover la acción de la justicia, defender la legalidad, los intereses del Estado y la Sociedad, representándolos conforme a lo establecido en la Constitución y en las Leyes de la República. Es único e indivisible y ejerce sus funciones a través de los fiscales, quienes lo representan íntegramente **[Ley Orgánica Ministerio Público, Bolivia]**

extracciones de datos en el momento (en la escena del hecho). Para que los otros peritos que acompañan al Ministerio Público en el acto puedan tomar los recaudos necesarios y permitir dichas actividades, previo el visto bueno de la autoridad competente que dá curso a la solicitud.

Estas solicitudes incluyen, según el caso la posibilidad de apertura de claves (en caso que se tenga información cifrada) por procedimientos informáticos si estas existen y el equipo no puede ser retirado, o bien el retiro parcial de algunas partes del equipo para que estas puedan, luego ser objeto de las pruebas periciales que se requieran.

El delito informatico de acuerdo al Art. 363 bis y 363 ter del Código Penal de Bolivia (ver Anexo B) debe producir daño o transferencia patrimonial. El perito informatico dirá sobre los aspectos técnicos, mas no podrá concluir sobre el daño o beneficio económico, para tal efecto necesitará considerar la figura de un perito contable o perito financiero quien en base a los datos e informacion validada por el perito informatico podrá decir sobre la cuantía del daño.



Para definir la selección del perito, se debe tomar en cuenta en primer lugar el ordenamiento legal que se tiene en nuestro país:

NCPP - BOLIVIA: Artículo 204º.- (Pericia).

Se ordenará una pericia cuando para descubrir o valorar un elemento de prueba sean necesarios conocimientos especializados en alguna ciencia, arte o técnica.

NCPP – BOLIVIA: Artículo 205º.- (Peritos).

I. Serán designados peritos quienes, según reglamentación estatal, acrediten idoneidad en la materia.

II. Si la ciencia, técnica o arte no está reglamentada o si no es posible contar con un perito en el lugar del proceso, se designará a una persona de idoneidad manifiesta.

III. Las reglas de este Título regirán para los traductores e intérpretes.

Más sobre los peritos y el ordenamiento legal vigente en nuestro país (ver Anexo F).

En un proceso penal, si la obtención de la evidencia digital afecta cualquier otro derecho constitucional o no es adecuada al cumplimiento de las garantías del debido proceso, dichas evidencias no pueden ser usadas en el juicio en contra del supuesto delincuente, lo que aumentaría notablemente la situación de impunidad que actualmente existe en materia de delitos informáticos o cometidos por medios informáticos, e incluso en delitos comunes donde la evidencia digital contenida en elementos electrónicos pudiere apoyar la investigación o condena de los criminales.

Bajo toda circunstancia se debe mantener la cadena de custodia (ver Anexo E), que es el mecanismo que garantiza la autenticidad de los elementos probatorios recolectados y analizados. Esto significa, que las pruebas correspondan al caso investigado sin que se dé lugar a confusión, adulteración, pérdida, ni sustracción alguna.

Por lo tanto, todo funcionario que participe en el proceso de cadena de custodia debe velar por la seguridad, integridad y preservación de dichos elementos.

La cadena de custodia garantiza que el perito informático reciba del investigador especial y/o fiscal, los elementos de prueba en el mismo estado en que fueron

colectados en la escena del hecho, igualmente que sean devueltos al investigador en la misma situación, que al ser presentados ante el tribunal se pueda comprobar su autenticidad y no existan dudas sobre la misma. Conforme lo dispuesto en el Art. 295 inciso 12 del Código de Procedimiento Penal vigente en nuestro país "Custodiar, bajo inventario, los objetos secuestrados" es decir toda transferencia de custodia debe quedar consignada en el Acta para Cadena de Custodia en el Caso de Delitos Informáticos (ver Figura 6, pág. 55) indicando: fecha, hora, nombre y firma de quién recibe y de quién entrega.

La naturaleza de los medios de almacenamiento digital, corren el riesgo de cambiar su estado o sufrir daños de transporte y conservación, debiendo la Fiscalia proveer las medidas para garantizar su permanencia en el tiempo, amparados en el Nuevo Código de Procedimiento Penal de Bolivia Art. 186.

NCPP - BOLIVIA: Artículo 186º.- (Procedimiento para el Secuestro)

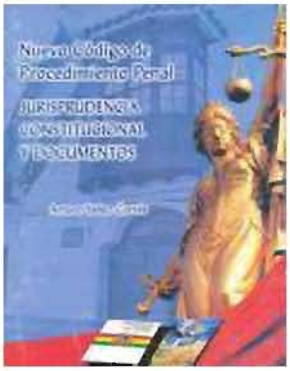
I. *Regirá el procedimiento establecido para el registro. Los objetos secuestrados serán inventariados y puestos bajo segura custodia en los depósitos de la Fiscalía o en los lugares especialmente destinados para estos efectos, bajo responsabilidad y a disposición del fiscal.*

II. Los semovientes, vehículos y bienes de significativo valor serán entregados a sus propietarios o a quienes acrediten la posesión o tenencia legítima, en calidad de depositarios judiciales después de realizadas las diligencias de comprobación y descripción.

III. *Si los objetos secuestrados corren riesgo de alterarse, desaparecer, sean de difícil conservación o perecederos, se ordenarán reproducciones, copias o certificaciones sobre su estado y serán devueltos a sus propietarios.*

Se podrá pedir el anticipo de prueba, si no existiesen garantías de traslado, es decir que no exista la seguridad de que al momento de realizarse el traslado la evidencia digital no sufra modificación alguna. Por ejemplo el riesgo de traslado es mayor en evidencias con componentes mecánicos que pueden dessincronizarce como en el caso de los Discos Duros.

NCPP - BOLIVIA: Artículo 307° (Anticipo de prueba)



I. Cuando sea necesario practicar un reconocimiento, registro, reconstrucción o pericia, que por su naturaleza o características se consideren como actos definitivos e irreproducibles, o cuando deba recibirse una declaración que, por algún obstáculo, se presuma que no podrá producirse durante el juicio, el fiscal o cualquiera de las partes podrán pedir al juez que realice estos actos.

II. El juez practicará el acto, si lo considera admisible, citando a todas las partes, las que tendrán derecho a participar con las facultades y obligaciones previstas en este Código.

III. Si el juez rechaza el pedido, se podrá acudir directamente al tribunal de apelación, quien deberá resolver dentro de las veinticuatro horas de recibida la solicitud, ordenando la realización del acto, si lo considera admisible, sin recurso ulterior.

En casos de evidencia digital, es recomendable que cuando no exista la posibilidad de garantizar un ambiente de conservación adecuado, la Fiscalia apoyada en el Artículo 307 del Nuevo Código de Procedimiento Penal de Bolivia, pueda generar medidas que garanticen la permanencia inalterable de la evidencia digital, ya que la preservación de la evidencia digital es vital, pues ésta es frágil y puede ser fácilmente alterada o destruida. Muchas veces esta alteración puede ser irreversible.

3.2.5.1 GARANTÍAS A CUBRIR

- ***El valor probatorio:***

En la realidad de los procesos penales, esta situación depende de la propia valoración que pueda dar el juez interviniente a las evidencias digitales que se aporten a la causa, de manera que cuanto mayor sea la información que pueda obtenerse de los equipos electrónicos que se catean y aseguran, mayor podrá ser la relevancia para una sentencia absolutoria o condenatoria según el caso de que se trate.

En realidad depende de un segundo factor que es la credibilidad que pueda tenerse en adquirir y conservar los equipos y la evidencia en ellos contenida, como así también en la inviolabilidad o no adulteración de esos contenidos a favor o en contra del sujeto a proceso.

- ***La inviolabilidad de los contenidos:***

De hecho este es en realidad el punto medular de la cuestión probatoria, ya que como se dijo, si la evidencia puede ser manipulada o es obtenida de forma ilegal, no sólo se corre el riesgo de que resulte inadmisible sino también de que con ella puedan caer partes importantes del proceso que podrían resultar en que un sujeto pudiera obtener su libertad aún cuando sea claramente responsable del hecho que se le imputa.

Teniendo en cuenta que es la representación social quien debe probar la culpabilidad, pues se presume la inocencia del encausado mientras no se pruebe su culpabilidad (*NCPP Art. 6º.- Presunción de Inocencia)* y sin las pruebas necesarias, o bien con ellas pero inadmisibles, esto resulta imposible para la parte acusadora quien vera disolverse sus posibilidades de manera directa al grado de errores en la búsqueda y recolección de bienes electrónicos.

NCPP - BOLIVIA: Artículo 6º.- (Presunción de Inocencia).

I. Todo imputado será considerado inocente y tratado como tal en todo momento, mientras no se declare su culpabilidad en sentencia ejecutoriada.

II. No se podrá obligar al imputado a declarar en contra de sí mismo y su silencio no será utilizado en su perjuicio.

III. La carga de la prueba corresponde a los acusadores y se prohíbe toda presunción de culpabilidad.

IV. En el caso del rebelde, se publicarán únicamente los datos indispensables para su aprehensión.

Los errores que se cometen son los que coadyuvan a la inadmisibilidad de las pruebas, siendo que a través de las cuales se podrían condenar o absolver a los indiciados, es imprescindible tratar de reducirlos al mínimo para que los elementos que puedan ser usados como prueba y la información que ellos contienen adquieran relevancia a la hora en que el decidor deba pronunciarse a través de la sentencia.

- ***La Privacidad :***

En procesos donde se involucre información contenida en equipos electrónicos, una de las garantías a cubrir es la privacidad, dado que si el sujeto titular de la información y en su caso propietario o poseedor del medio de soporte la colocó en ese formato, es para que no pueda ser accedida simplemente y sin su autorización expresa.

De hecho esta debemos tener presente que siempre es una garantía relativa, pues puede caer ante la orden expresa de un juez, pero siempre que se respeten los principios que le dan sustento, es decir que por ejemplo para la apertura de un correo electrónico se respeten las garantías que atañen a la comunicación postal.

En la Nueva Constitución Política del Estado (NCPE - Bolivia), el artículo más cercano al Habeas Data (Recurso para la protección de privacidad) se encuentra en:

NCPE - BOLIVIA: Artículo 130 (Acción de Protección de Privacidad)

I. *Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.*

II. *La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa.*

3.3 Demostración

3.3.1 Demostración de la Hipótesis

Las legislaciones y las instituciones judiciales han fundado sus bases sobre la admisibilidad de la evidencia en un proceso jurídico en cuatro conceptos (ver Apartado 2.1.4 Admisibilidad de la evidencia digital):

1) Autenticidad
2) Confiabilidad
3) Suficiencia
4) Conformidad con las leyes y reglas de justicia

En nuestro medio el cuarto concepto se enmarca en lo que es la "Conformidad con la legislación vigente en nuestro país".

Un razonamiento es deductivo si y solo si las premisas son evidencia de la verdad de la conclusión [Rojo, 1996], para tal efecto nos basaremos en el Razonamiento Deductivo Válido (ver Apartado 2.1.6.1.1)

Tenemos las siguientes premisas:
p = La evidencia digital es auténtica
q = La evidencia digital es confiable
r = La evidencia digital es suficiente
s = La evidencia digital está en conformidad con la legislación vigente en nuestro pais
t = La evidencia digital es admisible en un proceso jurídico

De lo cual obtenemos:

$$(p \wedge q \wedge r \wedge s) \rightarrow t$$

A continuación revisaremos cada uno de los cuatro conceptos (autenticidad, confiabilidad, suficiencia, conformidad con la legislación vigente en nuestro país) en

el Método Informatico Forense para el manejo adecuado de la evidencia digital y su admisibilidad en situaciones juridicas en nuestro país, desarrollado en la presente tesis.

3.3.1.1 Autenticidad

La autenticidad de la evidencia nos sugiere ilustrar a las partes en conflicto, que dicha evidencia ha sido generada y registrada en los lugares o sitios relacionados con el caso, particularmente en la escena del hecho o lugares establecidos en la diligencia de levantamiento de evidencia. Así mismo, la autenticidad, entendida como aquella característica que muestra *la no alterabilidad de los medios originales*, busca confirmar que los registros aportados corresponden a la realidad evidenciada. Éste concepto se puede apreciar claramente en todos los procedimientos:

En el procedimiento para identificar la evidencia digital a secuestrar (ver apartado 3.2.1) con la toma de fotografías, filmaciones del estado y posición de los equipos en la escena del hecho, el levantamiento del mapa de elementos informáticos involucrados se garantiza la autenticidad de la evidencia digital

En el procedimiento para adquirir la evidencia digital (ver apartado 3.2.2) se diferencian los componentes uno del otro por medio de etiquetas numeradas y firmadas, se realiza fotografías del número que se asigna a cada equipo.

Con la extracción original de datos (copia bit a bit) de la cual al obtenerse el valor hash existe un medio más para probar la autenticidad de la evidencia, además de las características de las evidencias, números de serie, el valor hash también se registra en el formulario de adquisición de evidencia digital, se realiza el precintado de los puertos y de componentes que puedan ser abiertos.

En el procedimiento para preservar la evidencia digital (ver apartado 3.2.3) la cadena de custodia es el mecanismo que garantiza la autenticidad de los elementos probatorios adquiridos y analizados. Esto significa, que las pruebas correspondan al

caso investigado sin que se dé lugar a confusión, adulteración, pérdida, ni sustracción alguna. Por lo tanto, todo funcionario que participe en el proceso de cadena de custodia vela por la seguridad, integridad y preservación de dichos elementos.

En el procedimiento para analizar la evidencia digital, el concepto de autenticidad se logra al realizar el análisis con herramientas forenses (con licencia).

En medios no digitales, la autenticidad de las pruebas aportadas no será refutada, de acuerdo por lo dispuesto en el Art. 216 del Nuevo Código de Procedimiento Penal :

NCPP-BOLIVIA: Artículo 216º.- (Documentos).

I. Se admitirá toda prueba documental lícitamente obtenida.

II. El imputado no podrá ser obligado a reconocer documentos privados que obren en su contra, debiendo el juez o tribunal interrogarle si está dispuesto a declarar sobre su autenticidad, sin que su negativa le perjudique. En este caso, las partes podrán acreditar la autenticidad por otros medios.

En el procedimiento para que la evidencia digital sea permitida legalmente se dan a conocer los aspectos legales que se debe considerar: presencia de un fiscal, orden judicial o requerimiento de un fiscal antes de empezar la aplicación del metodo informatico forense, se debe anotar todo lo que se realiza en el cuaderno de investigaciones, bajo constancia en el acta de allanamiento con la firma de todos los participantes y los testigos de actuación, para descartar que esa evidencia fue adquirida de manera ilegal y ademas para respaldar que fue levantada de la escena del hecho y autenticar que la evidencia proviene del incidente en cuestión.

Por todo lo expuesto anteriormente, el método informatico forense garantiza la autenticidad de la evidencia digital, de tal afirmación obtenemos la siguiente premisa:

p = La evidencia digital es auténtica

3.3.1.2 Confiabilidad

La confiabilidad de la evidencia digital, es otro factor relevante para asegurar la admisibilidad de la misma. La confiabilidad nos dice si efectivamente los elementos probatorios aportados *vienen de fuentes que son creíbles y verificables*, y que sustentan elementos de la defensa o del fiscal en el proceso que se sigue.

En el procedimiento para identificar la evidencia a secuestrar (ver apartado 3.2.1) con la realización de fotografías y filmaciones en la escena del hecho, levantamiento del mapa de elementos informáticos involucrados se garantiza la confiabilidad de la evidencia digital, pues es posible relacionar a la evidencia digital con el incidente ocurrido.

En el procedimiento para adquirir la evidencia digital (ver apartado 3.2.2) la extracción original de datos (copia bit a bit) y la obtención de los valores hash con herramientas forenses (con licencia) diseñadas con la finalidad de precautelar la confiabilidad de la evidencia digital, se evita todo tipo de susceptibilidades, éstas herramientas forenses también son utilizadas en el procedimiento para analizar la evidencia digital y al ser con licencia, no existe ninguna duda sobre las herramientas utilizadas.

En el procedimiento para que la evidencia digital sea permitida legalmente se respalda el concepto de confiabilidad con la presencia del fiscal en la escena del hecho; anotando en el cuaderno de investigación lo que se realiza y la constancia en el acta de allanamiento con la firma de todos los participantes y los testigos de actuación.

Por todo lo explicado, el método informatico forense garantiza la confiabilidad de la evidencia digital, de tal afirmación obtenemos la siguiente premisa:

q = La evidencia digital es confiable

3.3.1.3 Suficiencia

La suficiencia de la evidencia o más bien, la presencia de toda la evidencia es necesaria para adelantar el caso. Esta es una característica, que igual que las anteriores, es factor crítico de éxito en las investigaciones en procesos judiciales. Frecuentemente la falta de pruebas o insuficiencia de elementos probatorios ocasiona el retraso o terminación de procesos que podrían haberse resuelto. En este sentido, los abogados reconocen que mientras mayores fuentes de análisis y pruebas se tengan, habrá posibilidades de avanzar en la defensa o acusación en un proceso judicial.

En el procedimiento para identificar la evidencia a secuestrar, se busca identificar la mayor cantidad de evidencia pero que sea relevante al incidente, para que ésta pueda ser adquirida y de ésta forma las pruebas presentadas sean suficientes.

En el procedimiento para adquirir la evidencia digital (ver apartado 3.2.2), se toma en cuenta que no se espera que toda la información que se adquiera deba ser admisible como evidencia, pues mucha de esta información será utilizada para, a través de ella, descubrir evidencia admisible, es por eso que se trata de adquirir la mayor cantidad de evidencia de una escena del hecho bajo la supervisión y autorización de las autoridades competentes (Juez o Fiscal), para así poder mostrar el escenario completo, y no una perspectiva de un conjunto particular de circunstancias o eventos.

En el procedimiento para que la evidencia digital sea permitida legalmente, esta evidencia es suficiente siempre que cumpla la legalidad en la obtención de la misma, puesto que al ser tachada de ilegal automáticamente queda anulada.

Por tal motivo el método informatico forense garantiza la suficiencia de la evidencia digital, de ésta afirmación obtenemos la siguiente premisa:

r = La evidencia digital es suficiente

3.3.1.4 Conformidad con la legislación vigente en nuestro país:

En el procedimiento para que la evidencia digital sea permitida legalmente (ver apartado 3.2.5), se da a conocer la normativa sobre la cual debemos basarnos para aplicar éste método informatico forense, dicho procedimiento se rige en el Código Penal de Bolivia (Art. 363 Bis y 363 Ter), Nuevo Código de Procedimiento Penal de Bolivia y en la Nueva Constitución Política del Estado recientemente promulgada, es oportuno dar a conocer que nuestra legislación no tiene una normativa específica para garantizar que se cumplan las disposiciones legales con la finalidad de que la evidencia digital sea admisible.

Considerar que cuando se tiene acceso a la evidencia digital por medios no autorizados, las mismas son tachadas de ilegales y no existen vías para probar su autenticidad, confiabilidad y suficiencia. La evidencia debe ser obtenida de manera legal, es por eso que se hace tanto énfasis en contar desde el principio con la orden judicial o requerimiento de un fiscal antes de empezar con la aplicación del metodo informatico forense.

Además los procedimientos para identificar la evidencia a secuestrar, adquirir, preservar y analizar la evidencia digital están enmarcados en el "Procedimiento para que la evidencia digital sea permitida legalmente", púes todo lo que se realice con la evidencia digital debe estar en conformidad con la legislación vigente de nuestro país; de esta forma cumplir con el cuarto concepto requerido para la admisibilidad de la evidencia digital.

De lo expuesto en éste apartado, el método informatico forense garantiza que la evidencia digital esté en conformidad con la legislación vigente en nuestro país, por tal afirmación obtenemos la siguiente premisa:

s = La evidencia digital está en conformidad con la legislación vigente en nuestro país

Por los planteamientos expuestos en los apartados (3.3.1.1, 3.3.1.2, 3.3.1.3 y 3.3.1.4), se afirma que el método informatico forense para el manejo adecuado de la evidencia digital y su admisibilidad en situaciones jurídicas en Bolivia, garantiza de la evidencia digital la autenticidad, confiabilidad, suficiencia y conformidad con la legislación vigente en nuestro país, de ésta afirmación obtenemos:

$(p \wedge q \wedge r \wedge s)$

Por la Regla de Inferencia del Modus Ponens del Razonamiento Deductivo Válido (ver apartado 2.1.6.1.1), tenemos:

$(p \wedge q \wedge r \wedge s)$ // Del método informatico forense de ésta tesis

$\underline{(p \wedge q \wedge r \wedge s) \rightarrow t}$ // De las bases sobre la admisibilidad de la evidencia (σ)

t // La evidencia digital es admisible

Para nuestro caso $u = (p \wedge q \wedge r \wedge s)$ ***Modus Ponens:*** $\dfrac{u \qquad u \rightarrow t}{t}$

Tabla de Verdad:

u	t	[u	^	(u→t)]	⟶	t
V	V	V	V	V	V	V
V	F	V	F	F	V	F
F	V	F	F	V	V	V
F	F	F	F	V	V	F
		(1)	(3)	(2)	(5)	(4)

Tabla 1: Comprobación de Tautología
Fuente: Elaboración Propia

(σ) Analizado al principio de la "demostración de la hipótesis" el cual está sustentado en la investigación realizada por el Dr Jeimy Cano especialista en Derecho Informático Penal

Por lo tanto, como (5) es una tautología, queda demostrado que éste razonamiento es válido.

Con lo cual se concluye que el método informatico forense garantiza la admisibilidad de la evidencia digital en situaciones jurídicas en nuestro país, púes si se maneja adecuadamente la evidencia digital de manera que se mantenga su autenticidad, confiabilidad, suficiencia y conformidad con la legislación vigente en nuestro país, la evidencia digital llega a ser admisible en un proceso jurídico.

CAPÍTULO 4
CONCLUSIONES Y RECOMENDACIONES

CAPITULO 4

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Se construyó el procedimiento para identificar la evidencia a secuestrar, con lo cual se logra el primer objetivo específico, éste se encuentra en el apartado 3.2.1.

- El procedimiento que se encuentra en el apartado 3.2.2 permite lograr el objetivo específico de adquirir la evidencia digital.

- De la misma forma se realizó el procedimiento para preservar la evidencia digital el cual se encuentra en el apartado 3.2.3, que permite alcanzar el tercer objetivo específico.

- Se logró el objetivo específico de proponer un procedimiento para analizar la evidencia digital, mismo que se encuentra en el apartado 3.2.4.

- También se elaboró del procedimiento para que la evidencia digital sea permitida legalmente, dicho procedimiento se encuentra en el apartado 3.2.5, éste nos permite alcanzar el último objetivo específico.

- La elaboración de todos éstos procedimientos y la consecución de los mismos, ayuda a lograr el objetivo general, planteado como: "desarrollar y proponer un método informático forense que permita manejar adecuadamente la evidencia digital, mantener de los elementos probatorios la autenticidad, confiabilidad, suficiencia, conformidad con leyes y reglas de justicia y así garantizar la admisibilidad de la misma en situaciones jurídicas."

- Habiendo logrado el objetivo general y además demostrada la hipótesis, se concluye que se ha resuelto el problema, puesto con un Método Informático Forense se puede lograr que exista un manejo adecuado de la evidencia digital, que permita garantizar de los elementos probatorios la autenticidad, confiabilidad, suficiencia, conformidad con leyes y reglas de justicia, y así hacer que ésta evidencia sea admisible en un proceso jurídico.

4.2 Recomendaciones

Profundizar temas referentes a informatica forense, pues siendo ésta una nueva disciplina hace falta investigar y ampliar nuestros conocimientos en ésta área.

Se recomienda proponer métodos informáticos forenses tomando en cuenta la perspectiva de ser aplicado en las áreas de network forensics (forensia en redes) y digital forensics (forensia digital), también se propone realizar un método informático forense que permita preservar la evidencia digital después que la misma haya sido considerada admisible en un proceso jurídico.

Los campos mencionados pueden llegar a ser fuentes muy interesantes de estudios.

Además se sugiere a las autoridades de la Carrera de Informática gestionar la creación de una nueva mención dentro del pensúm, pues es necesaria la formación de profesionales en el área de Informática Forense, ya que hasta la fecha en nuestra carrera se opta al Titulo de Licenciatura en Informática con Mención en Ingeniería de Sistemas Informáticos y con Mención en Ciencias de la Computación, sería un gran avance que se pueda optar al "Titulo de Licenciatura en Informática con Mención en Informática Forense".

GLOSARIO DE TERMINOS

A

Acta: Documento en el que se hace constar determinado acto judicial.

Allanar: Una de las acepciones de este verbo es registrar, inspeccionar, otro significado es irrumpir, entrar, penetrar.

Allanamiento: Es una medida judicial y consiste en ingresar en un sitio sin la voluntad del dueño u ocupante. La diligencia es realizada en forma personal por el magistrado o encomendada a funcionarios de policía mediante una orden de allanamiento

C

Ciencia Forense

La definición del diccionario de ciencia forense es la aplicación de prácticas científicas dentro del proceso legal. Esencialmente esto se traduce en investigadores altamente especializados (peritos) o criminalistas, que localizan evidencias que sólo proporcionan prueba concluyente al ser sometidas a pruebas en laboratorios. Parte de la evidencia que se halla a menudo no puede ser vista a simple vista, a veces es hasta más pequeña o incluso es intangible como en el caso de las investigaciones realizadas en informática forense.

D

Delito: Acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena.

Delito Informático: Son aquellos actos delictivos realizados con el uso de computadoras o medios electrónicos, cuando tales conductas constituyen el único medio de comisión posible –o el considerablemente más efectivo-, y los delitos en

que se daña estos equipos, redes informáticas, o la información contenida en ellos, vulnerando bienes jurídicos protegidos. [Wikipedia, 2008].

Disco Compacto: Dispositivo de almacenamiento masivo, comúnmente de plástico recubierto con láminas de diferente material. De acuerdo con su formato de grabación, sus características físicas, de capacidad y la densidad de datos almacenados se los denomina CDs o DVDs. Pueden ser regrabables.

Disco Duro: Dispositivo de almacenamiento masivo, comúnmente superficie metálica magnetizada. Se considera el objeto de mayor relevancia por contener la mayor cantidad de información que puede ser considerada como evidencia. Son regrabables.

Disco Flexible: Dispositivo de almacenamiento reducido, comúnmente llamado diskette. De plástico recubierto con una lámina magnética.

E

Escena del hecho: Lugar donde se suscitó el delito informático de donde se obtendrán las evidencias digitales.

e_locard: Principio sobre el intercambio entre dos cuerpos que entran en contacto, se afirma que ambos intercambian algo en el proceso. Cuando 2 dispositivos electrónicos se comunican intercambian datos siguiendo un protocolo, el rastro queda almacenado y dependiendo del tipo de almacenamiento podemos encontrarlo posterior al proceso de intercambio.

Evidencia: Etimológicamente proviene del latín Evidentia. Cualidad de evidente (Cierto, claro, sin duda), Certeza clara y manifiesta de la que no se puede dudar.

Evidencia digital: Cualquier objeto, archivo, fotografía u otro que tenga estrecha relación o este realizado mediante soporte informático, el cual se encuentre vinculado con algún delito, que posteriormente es recolectado de una escena del hecho.

"Información de valor probatorio almacenada o transmitida en forma digital" IOCE (Internacional Organization of Computer Evidence)

Se trata de demostrar una entrada, existencia, copia, etc., que haya sido realizado usando medios informáticos, presenta particularidades no conceptuales sino directamente relacionadas con el medio físico que la soporta, el cual al ser electrónico, magnético u óptico puede sufrir alteraciones, modificaciones o simplemente daños permanentes al ser apagado, trasladado, encendido o cualquier otra acción casual o intencionada. [Rosales, 2008]

M

Memorias USB (*Universal Serial Bus):* Es un pequeño dispositivo de almacenamiento que utiliza memoria flash para guardar la información, estas memorias son resistentes a los rasguños (externos) al polvo y algunos al agua. Existen con capacidades en memoria de 1, 2, 4, 8, 16, 32, 64, 128 GB.

Ministerio Público: Órgano constitucional que tiene por finalidad promover la acción de la justicia, defender la legalidad, los intereses del Estado y la Sociedad, representándolos conforme a lo establecido en la Constitución y en las Leyes de la República. Es único e indivisible y ejerce sus funciones a través de los fiscales, quienes lo representan íntegramente. [Ley Orgánica Ministerio Público, Bolivia]

O

Orden: Mandato superior que se debe obedecer y ejecutar por los inferiores.

P

Pericia: Sabiduría, experiencia y habilidad en una ciencia o arte.

Pericial: Relativo al perito o al peritaje.

Permitida Legalmente: Evidencia que fue obtenida de manera legal.

Precintar: Poner cinta especial para no permitir que las evidencias sean manipuladas y dañadas por terceras personas

R

Relevante: Relacionada con el crimen bajo investigación.

Requerimiento de Fiscal: Documento que envía la autoridad fiscal a un determinado individuo.

S

Secuestrar: Embargo de una cosa o de un bien por orden judicial. En informática forense éste término indica que se debe sustraer la evidencia digital del lugar donde aconteció dicho delito.

Suficiencia: Se usa esta palabra para hacer referencia a que se aportan todas las evidencias pertinentes al caso.

Swap: En informática, al espacio de intercambio de un disco.

T

Trazabilidad: Capacidad de seguimiento y reconstrucción de acciones efectuadas por los usuarios en un sistema.

Bibliografía

[Access Data, 2008] Access Data: Forensic Toolkit Consultado el 9 de Septiembre de 2008 en la WWW: www.accessdata.com/media/es_MX/print/brochures/AD.ProdBrochure.es_MX.pdf

[Cano, 2003a] Cano, Jeimy J. (2003). Admisibilidad de la Evidencia Digital: Algunos elementos de revisión y análisis. *Revista de Derecho Informatico Alfa-Redi*. Consultado el 22 de octubre de 2008 en la WWW: http://www.alfa-redi.org

[Cano, 2003b] Cano, Jeimy J. (2003). Introducción a la Informatica Forense. *Revista de Derecho Informatico Alfa-Redi*. Consultado el 28 de octubre de 2008 en la WWW: http://www.alfa-redi.org

[Caracciolo] Caracciolo, Claudio B. (n.d.). I Jornada: "Tecnología, Integración.. ... ¿Seguridad?". Consultado el 14 de octubre de 2008 en la WWW: www.ona.gob.ve/Vision360/Presentaciones/CCaracciolo.pdf

[Casey, 2001] Casey, E. (2001) Handbook of Computer Crime Investigation. Academic Press.

[Código Penal, 1999] Ley del Código Penal. Ley No. 1970, Ley Del 25 De Marzo de 1999, Hugo Banzer Suarez, Presidente de la Republica de Bolivia.

[Dávila, 2006] Dávila, Gladys (2006). El Razonamiento Inductivo y Deductivo Dentro del Proceso Investigativo en Ciencias Experimentales y Sociales. *Revista de Educación Laurus*, vol 12, 184 - 189.Universidad Pedagógica Experimental Libertador Caracas de Caracas – Venezuela. Consultado el 10 de noviembre de 2008 en la WWW: http://redalyc.uaemex.mx/redalyc/pdf/761/76109911.pdf

[Guidance Software, 2008] Guidance Software Consultado el 9 de septiembre de 2008 http://www.guidancesoftware.com/products/ef_index.asp

[IOCE, 2000] IOCE. (2000) Elements for testing of internet investigators. IOCE – International Organization on Computer Evidence. IOCE 2000 Conference. http://www.ioce.org/.

[Inza, 2006] Inza, Julián(2006).Consultado el 9 de septiembre de 2008 en WWW: inza.wordpress.com/2006/11/26/herramientas-de-informatica-forense-para-memorias-usb/ - 96k

[Ley Orgánica Ministerio Público, Bolivia] Ley Orgánica del Ministerio Público. Ley Nº 2175. Honorable Congreso Nacional de Bolivia.

[Mckemmish, 1999] Mckemmish, R (1999). What is forensic computing?. *Australian Institute of Criminology*. Issues and Trenes in crime and criminal justice. No. 118.

[Reino, 2007] Reino, Alfredo (2007, octubre). Informática Forense (II). Práctica de análisis forense. Consultado el 10 de agosto de 2008 en la WWW: http://www.areino.com/forensics-2/

[Restrepo, 2007] Restrepo, Ana María (2007, junio). Computación Forense, Análisis de "Cadáveres" Virtuales. *Comunnity CXO*. Consultado el 9 de septiembre de 2008 en la WWW: http://www.dragonjar.org/computacion-forense-analisis-de-cadaveres-virtuales.xhtml

[Rojo, 1996] Rojo, Armando O. (1996) Lógica- Razonamiento Deductivo Válido, Algebra I- 18ª. ed.- Buenos Aires: El Ateneo

[Rosales, 2008] Rosales, Guido E. (2008, septiembre) Ingeniero de sistemas y Master en Ciencias de la Ingeniería, especialista en seguridad informatica. Seminario INFOFOR sobre Informatica Forense , La Paz – Bolivia, 19-20 septiembre, (paper).

[Standards Australia International, 2003] Standards Australia International (2003) HB171:2003 Handbook Guidelines for the management of IT evidence.

[Sommer, 1995] Sommer, P. (1995) Forensic Computing – CSRC Research Project. http://csrc.lse.ac.uk/People/sommerp/forensic.htm

[Torres et al., 2006] Torres, Daniel A.; Cano, Jeimy J. y Rueda, Sandra J. (2006, noviembre). Procedimiento forense para el manejo de investigaciones. Evidencia digital en el contexto colombiano. *Revista ACIS*. Consultado el 14 de septiembre de 2008 en la WWW: http://www.acis.org.co/index.php?id=856

[Velásquez, 2008] Velásquez, Andrés (2008, junio). Conversaciones e ideas sobre negocios y nuevas tecnologías. Entrevista sobre computo forense. *Radio Eón 4.5 Frecuencia Cero por Antonio Quirarde*. México.

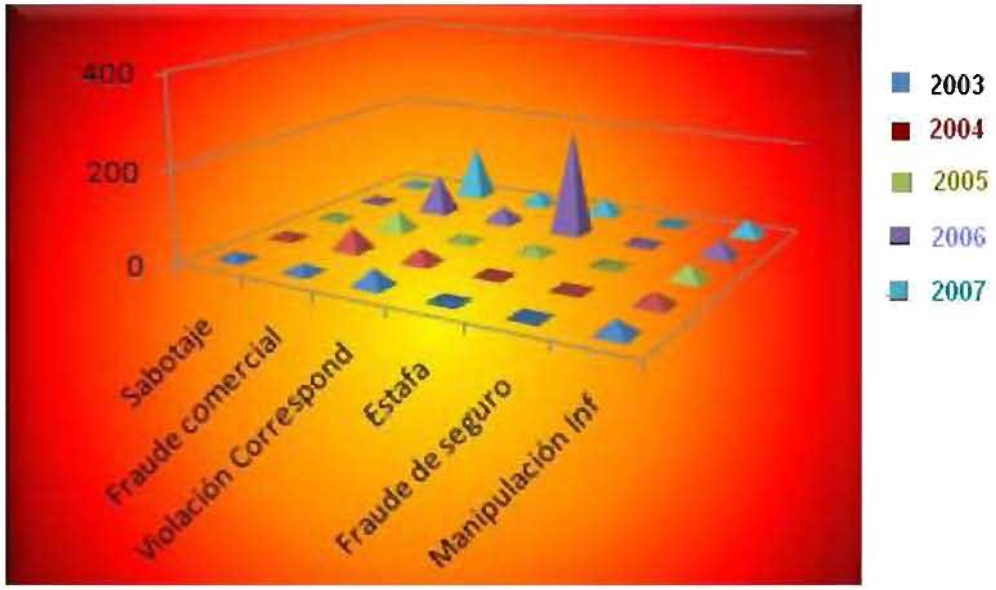
[Wikipedia, 2008] Wikipedia (2008).Delitos Informáticos. Consultado el 5 octubre de 2008 en la WWW: http://es.wikipedia.org/wiki/Delitos_inform%C3%A1ticos

ANEXOS

ANEXO A

Estado de los Delitos Informáticos en Bolivia
"Estadísticas Nacionales"

CASOS REGISTRADOS POR AÑOS



FUENTE: FELCC

Seminario INFOFOR

La Paz – Bolivia, 19 de septiembre de 2008 (paper)

ANEXO B

CÓDIGO PENAL DE BOLIVIA
DELITOS INFORMÁTICOS

Artículo 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 un tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

Artículo 363.- Ter (Alteración acceso y uso indebido de datos informáticos). El que sin estar autorizado apoderare, 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."[Código Penal, 1999].

ANEXO C

Aspecto Metodológico

Tipo de Estudio Exploratorio

La Informatica Forense al ser una disciplina que recién se está practicando, tiene muchas carencias en cuanto respecta a métodos, metodologías y bases bibliográficas, por ésta situacion su aplicación es muy restringida, es por eso que se propone el desarrollo de un método informatico forense para el manejo adecuado de la evidencia digital, con la finalidad de aportar bases sólidas para la aplicación practica de ésta rama de la Informática.

Ésta especialidad no es muy conocida en nuestro medio y en nuestra carrera no se tiene ningún antecedente referente a Informatica Forense y menos aún sobre algún método utilizado en la aplicación de la misma, lo cual indica que no se ha realizado otros estudios sobre éste tema y por eso se quiere profundizar más, para dar a conocer una base sólida a nuestra sociedad en su conjunto.

Cómo no se cuenta con muchas bases teóricas, se pretende recopilar informacion del tipo teórico de las pocas que existen de revistas, artículos científicos, entrevistas a profesionales especialistas en ésta área es decir realizar una investigación profunda y desarrollar un método informatico forense que permita el manejo adecuado de la evidencia digital y posibilite la admisibilidad de la misma en situaciones juridicas.

Con el método informatico forense para el manejo adecuado de la evidencia digital, se pretende dar confianza a los profesionales informáticos para que puedan realizar una aplicación correcta de la Informatica forense al tratar con delitos donde se haya utilizado soporte informatico, manejando la evidencia digital de manera adecuada, lo cual posibilita la admisibilidad de la evidencia digital en situaciones juridicas, misma que conduce al castigo de conductas impropias y por ende al ser castigado éstos delitos otro individuo que quiere emprender en estas conductas reprochables lo dudará antes de convertirse en un delincuente.

ANEXO D

HERRAMIENTAS FORENSES

Las herramientas informáticas, son la base esencial de los análisis de las evidencias digitales en los medios informáticos. Sin embargo, éstas requieren de una formalidad adicional que permita validar tanto la confiabilidad de los resultados de la aplicación de las mismas, como la formación y conocimiento del investigador (informático forense) que las utiliza.

Características de las herramientas de recolección forenses [Torres et al., 2006]
Las características técnicas mínimas que deben cumplir las herramientas forenses para que la evidencia recolectada y/o analizada por ellas sea confiable son las siguientes:

- Manejar diferentes niveles de abstracción: dado que el formato de la información en su nivel más bajo es difícil de leer, la herramienta debe interpretar la información y ofrecer acceso en diferentes niveles.

- Deben tener la capacidad de extraer una imagen bit a bit de la información. Todo byte debe ser copiado de la fuente, desde el comienzo hasta el final de ella sin importar si hay fragmentos en blanco.

- Deben tener un manejo robusto de errores de lectura. Si el proceso de copia falla al leer un sector del medio fuente, se debe marcar en el medio destino un sector del mismo tamaño y en la misma ubicación que identifique el sector que no pudo leerse, adicionalmente estas fallas deben ser documentadas.

- La aplicación no debe cambiar de ninguna manera el medio original, debe tener la habilidad de realizar pruebas y análisis de una manera científica. Estos resultados deben poder ser reproducibles y verificables por una tercera persona.

Las herramientas utilizadas actualmente en informática forense están cumpliendo una función importante para esclarecer los hechos ante incidentes informáticos, a continuación se dan a conocer algunas herramientas que son utilizadas en la aplicación de la informatica forense [Fernández, 2004]. El uso de herramientas para tratar la evidencia es tanto en ámbito de hardware y software:

HARDWARE

Se mencionan equipos especializados en identificación biométrica como en captura de evidencias.

• Como Identificación biométrica: Usados para autenticar la identidad de un usuario a través de un atributo o rasgo único. Esto generalmente implica el uso de un lector. Algunos tipos:

a)Huella Digital
b)Análisis de palma
c)Iris, retina
d)Rostro
e)Reconocimiento de Voz

• Como captura de evidencias: Brindan la posibilidad de recopilar evidencias (copias) preservando las características y detalles de la evidencia original. Por ejemplo tenemos:

a) DIBS RAID: Dispositivo de hardware de una sola vía, para realizar copias forenses de disco a disco.
Es necesario abrir el computador y manipular el disco sospechoso.

b) DIBS PERU

Realiza las copias en cartuchos ópticos, que permite hacer copias sin necesidad de conectar directamente el disco sospechoso al dispositivo. No se manipula directamente el disco duro sospechoso.

c) ICS Products

Estos dispositivos duplican el disco duro dañado y trabajan con éste. Al analizarlo, a través de un "booteo" se acceden a los datos.

• NOTA: Un caso especial, que no encaja en los casos anteriores, es para una herramienta que controla y monitorea el uso de una computadora, se trata del KeyLogger.

El Keylogger viene a ser una aplicación que almacena las pulsaciones sobre el teclado, siendo ésto guardado en un archivo o en mail, con información sobre el proceso, hora , fecha, mensajes de la aplicación, etc. El usuario no se dará cuenta del uso de esta herramienta, ya que trabaja en modo oculto.

SOFTWARE

Existe software forense que opera creando una copia de respaldo de la información a analizar. Tenemos por ejemplo:

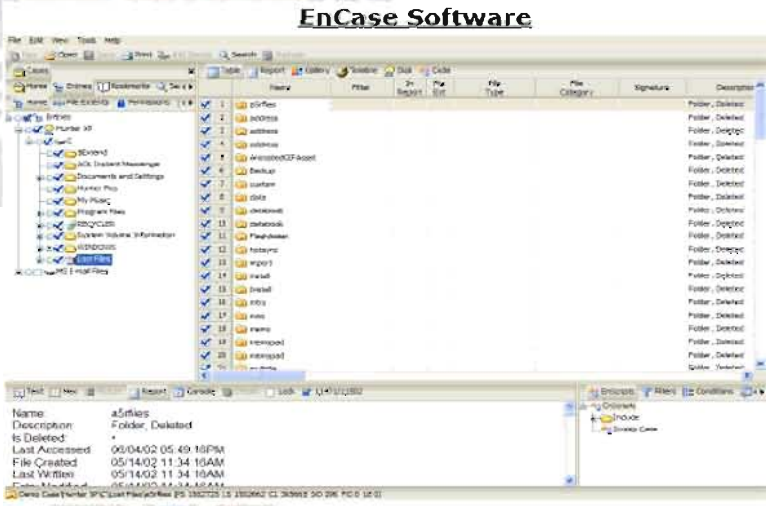
a) EnCase Forensic [Guidance Software, 2008]:

Software líder en el mercado, de mayor uso en el ámbito de análisis forense. EnCase Forensic le proporciona las herramientas para investigar y documentar con éxito muchos delitos locales internos (pornografía infantil, violencia doméstica, acoso, drogas, apuestas y robo de identidad), sin omitir evidencia informática valiosa o tener que esperar laboratorios con trabajo atrasado. La solución permite a los examinadores investigar la evidencia dentro de una sola interfaz gráfica, mediante el

uso de un grupo de herramientas, que reduce drásticamente el tiempo que los investigadores emplean en casos individuales.

Desarrollado por expertos en análisis forense penal, EnCase Forensic cuenta con la aprobación de tribunales de justicia de todo el mundo. El software sigue siendo la herramienta elegida por el FBI, el Departamento de Seguridad Nacional de Estados Unidos (US Department of Homeland Security), el Departamento de Defensa de Estados Unidos (US Department of Defense), New Scotland Yard y miles de laboratorios criminalistas y agencias encargadas del cumplimiento de la ley en todo el mundo.

EnCase Forensic permite que los investigadores manejen fácilmente grandes volúmenes de evidencia informática al visualizar todos los archivos relevantes, incluidos los archivos "eliminados", los espacios muertos de los archivos y los espacios no designados.



Además proporciona las adquisiciones de medios con más validaciones de la industria. La solución crea un duplicado binario exacto de la unidad o disco original y luego lo verifica al generar valores hash MD5 para archivos de imágenes relacionados. Además, EnCase asigna valores de control de redundancia cíclica a los datos a fin de revelar las instancias en que las pruebas se modificaron forzosamente o se alteraron de alguna manera. Este enfoque fue validado por el Instituto Nacional de Normas y Tecnología (National Institute for Standards and Technology, NIST) y resistió numerosos cuestionamientos por parte de los tribunales de justicia.

Características de EnCase:

- *Útiles vistas de gráficos*

Vistas de línea de tiempo expandida

Muestra de forma instantánea una gran variedad de medios o gráficos informáticos. Es compatible con los formatos ART, BMP, GIF, JPG, PNG y TIFF.

- *Vistas de línea de tiempo expandida*

Proporciona una vista calendario de todas las actividades en los archivos, que muestra cuándo se crearon los archivos o cuándo se produjo el último acceso o la última escritura. El calendario alterna meses y años para ayudar a los examinadores a ver los patrones de la actividad en los archivos.

- Opciones de adquisición flexibles

Brinda la posibilidad de obtener imágenes de medios con sistemas operativos múltiples, lo que genera flexibilidad y ahorra tiempo en casos de adquisiciones difíciles. La solución admite la obtención de imágenes en Windows, DOS y Linux y presenta diversas opciones de compresión, velocidad y manejo de errores.

- *Informes detallados*

Genera información detallada sobre archivos, carpetas, volúmenes, discos duros y casos específicos. Permite visualizar datos referidos a la adquisición de datos, la geometría de la unidad, las estructuras de las carpetas y las imágenes y los archivos marcados. Exporta informes en formato RTF o HTML.

Genera reporte del proceso, mostrando el caso investigado, la evidencia principal, algunos comentarios, imágenes recuperadas, tiempo en que se realizó la búsqueda.

- *Otras Características*

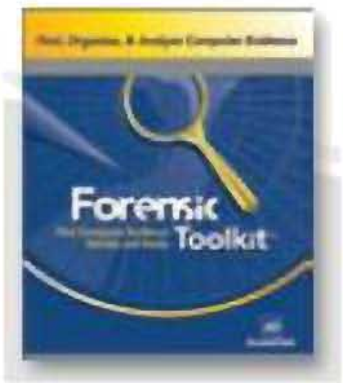
-Soporte multiplataforma: Windows, Solaris, Macintosh, Linux.

-Crea copias comprimidas de los discos fuente para poder analizarlo, buscarlo y verificarlo.

-Proporciona y documenta eficientemente fechas, horas, registros de accesos, es decir todos los rastros de intervención en un proceso.

-Permite ver archivos borrados, ocultos. EnCase localiza automáticamente y despliega muchos formatos de imágenes, incluyendo las que fueron eliminadas. De todas estas se escogen las imágenes más relevantes para el caso.

b) Forensic Toolkit [Access Data, 2008]:



Es una suite de herramientas para el análisis de las propiedades o especificaciones de ficheros. Examina los ficheros de un disco en busca de actividad no autorizada y los lista por su última fecha de acceso, permitiendo realizar búsquedas en franjas horarias, búsqueda de archivos eliminados y data streams (utilizados para ocultar información en sistemas NT/2K). Obtener atributos de seguridad de ficheros.

Forensic Toolkit de AccessData (FTK) ofrece a los profesionales encargados de controlar el cumplimiento de la ley y a los profesionales de seguridad la capacidad de realizar exámenes forenses informatizados completos y exhaustivos. FTK posee funciones eficaces de filtro y búsqueda de archivos. Los filtros personalizables de FTK permiten buscar en miles de archivos para encontrar rápidamente la prueba que necesita. FTK ha sido reconocida como la mejor herramienta forense para realizar análisis de correo electrónico.

FÁCIL DE USAR

- La tecnología Outside In Viewer de Stellent le permite ver cientos de formatos de archivos
- FTK Imagen le permite navegar rápidamente por las imágenes adquiridas

- Genere registros de auditoría e informes del caso
- Es compatible con Password Recovery Toolkit y Distributed Network Attack

OPCIONES DE BÚSQUEDA AVANZADAS

- Búsqueda en el índice de texto completo suministrada por dtSearch muestra los resultados de búsqueda de texto al instante
- Restauración de datos avanzada para textos de Internet, gráficos, documentos de MS Office entre otros
- Encuentre patrones binarios con Live Search(Búsqueda directa)
- Encuentre archivos importantes rápidamente mediante la creación de filtros de archivos personalizados

REGISTRY VIEWER

- Analice la información de cuenta, como nombres de usuarios y contraseñas, de Internet Explorer, Outlook y Outlook Express
- Abre todas las versiones de archivos de registro de Windows
- Se integra fácilmente con los informes del caso de Forensic Toolkit

ANÁLISIS DE CORREO ELECTRÓNICO Y DE ARCHIVOS ZIP

- Permite: correo electrónico de Outlook, Outlook Express, AOL, Netscape, Yahoo, Earthlink, Eudora, Hotmail y MSN
- Vea, busque, imprima y exporte mensajes y archivos adjuntos de correo electrónico
- Recupere mensajes de correo electrónico borrados parcial o totalmente
- Extraiga datos automáticamente desde archivos comprimidos PKZIP, WinZip, WinRAR, GZIP y TAR

ARCHIVOS Y FORMATOS DE ADQUISICIÓN ADMITIDOS

- Los formatos de archivos incluyen: NTFS, CDFS, UDF, HFS, FAT 12/16/32 y Linux EXT2 & EXT3
- FTK y FTK Imager pueden leer formatos de imágenes de EnCase, SMART, Symantec, Linux DD entre otros

Además que permite:

-Análisis de punta, permite descrifrar y crackear password.

-El uso de una base de datos para manejar su información obtenida.

c) SafeBACK:

Aplicación usada para crear "imágenes espejo" de disco duro (completo o partición).

Algunas características que presenta:

-Basado en DOS ya que Windows puede alterar los datos.

-Indaga la existencia de archivos ocultos cuando los sectores no presentan semejanza con el enlace de disco duro.

-Copia al 100% todas las áreas del disco duro.

El acceso a las memorias USB plantea interesantes retos para los analistas forenses. Herramientas como SafeBack permiten hacer copias exactas de diferentes tipos de memorias (como las que se emplean en las cámaras de fotos digitales) a nivel de bit. Es necesario tener un interfaz fiable para estos tipos de memorias, por lo que es conveniente seleccionar un poco. En el caso de los "lápices" o "llaves" USB el interfaz va incorporado en el dispositivo [Inza, 2006].

ANEXO E

CADENA DE CUSTODIA [Reino, 2007]

La cadena de custodia es el mecanismo que garantiza la autenticidad de los elementos probatorios recolectados y examinados. Esto significa, que las pruebas correspondan al caso investigado sin que se dé lugar a confusión, adulteración, pérdida, ni sustracción alguna. Por lo tanto, todo funcionario que participe en el proceso de cadena de custodia debe velar por la seguridad, integridad y preservación de dichos elementos.

El objetivo de la cadena de custodia consiste en mantener un registro de todas las operaciones que se realizan sobre la evidencia digital en cada uno de los pasos de investigación de manera detallada.

Esta expresión es un término legal que se refiere a la capacidad de garantizar la identidad e integridad de un espécimen o evidencia desde su obtención, durante su análisis y hasta el final del proceso.

En la práctica consiste en salvaguardar la evidencia, de forma documentada, de forma que se eviten alegaciones de que la evidencia ha sido modificada o alterada durante el proceso de la investigación.

Con los objetos físicos que constituyen evidencia, la práctica es almacenarlos en bolsas o sobres sellados, con un formulario que especifica quién ha recogido la evidencia y cada persona que la haya usado para algo, de forma que no quede duda sobre quién ha tenido acceso a ella y cuándo.

Con la evidencia electrónica (imágenes de discos y memoria, ficheros de datos y ejecutables, etc.) la práctica consiste en obtener "hashes" de la información en el momento de su recolección, de forma que se pueda comprobar en cualquier momento si la evidencia ha sido modificada.

ANEXO F

NUEVO CODIGO DE PROCEDIMIENTO PENAL DE BOLIVIA

(NCPP – BOLIVIA)

NCPP - BOLIVIA: **Artículo 208º.- (Impedimentos).**

No serán designados peritos los que hayan sido testigos del hecho objeto del proceso y quienes deban o puedan abstenerse de declarar como testigos.

NCPP - BOLIVIA: **Artículo 209º.- (Designación Y Alcances).**

I. Las partes podrán proponer peritos, quienes serán designados por el fiscal durante la etapa preparatoria, siempre que no se trate de un anticipo jurisdiccional de prueba, o por el juez o tribunal en cualquier etapa del proceso.

II. El número de peritos será determinado según la complejidad de las cuestiones por valorarse.

III. El fiscal, juez o tribunal fijarán con precisión los temas de la pericia y el plazo para la presentación de los dictámenes. Las partes podrán proponer u objetar los temas de la pericia.

NCPP - BOLIVIA: **Artículo 210º.- (Excusa Y Recusación).**

Los peritos podrán excusarse o ser recusados por los mismos motivos establecidos para los jueces. El juez o tribunal resolverá lo que corresponda, previa averiguación sumaria sobre el motivo invocado sin recurso ulterior.

NCPP - BOLIVIA: **Artículo 211º.- (Citación Y Aceptación Del Cargo).**

I. Los peritos serán citados en la misma forma que los testigos. Tendrán el deber de comparecer y desempeñar el cargo para el cual fueron designados, previo juramento o promesa. Si tuvieran impedimento o no fueran idóneos deberán poner en conocimiento del fiscal, juez o tribunal, para que previa averiguación sumaria, resuelva lo que corresponda, sin recurso ulterior.

II. Rige, la disposición del Artículo 198º de este Código.

NCPP - BOLIVIA: **Artículo 198º.- (Compulsión).**

Si el testigo no se presenta a la primera citación, se expedirá mandamiento de aprehensión, sin perjuicio de su enjuiciamiento. Si después de comparecer se niega a declarar se dispondrá su arresto, hasta por veinticuatro horas, al término de las cuales, si persiste en su negativa se le iniciará causa penal.

NCPP - BOLIVIA: **Artículo 212º.- (Ejecución).**

I. El juez o tribunal, resolverá todas las cuestiones que se planteen durante las operaciones periciales y brindará el auxilio judicial necesario.

II. Si existen varios peritos, siempre que sea posible, practicarán juntos el examen. Las partes y sus consultores técnicos podrán asistir a la pericia y pedir las aclaraciones pertinentes, debiendo retirarse cuando los peritos comiencen la deliberación.

III. El fiscal, juez o tribunal ordenará la sustitución del perito que no concurra a realizar las operaciones periciales dentro del plazo fijado o desempeñe negligentemente sus funciones.

IV. El perito deberá guardar reserva de todo cuanto conozca con motivo de su actuación.

NCPP - BOLIVIA: **Artículo 213º.- (Dictamen).**

I. El dictamen será fundamentado y contendrá de manera clara y precisa la relación detallada de las operaciones practicadas y sus resultados, las observaciones de las partes o de sus consultores técnicos y las conclusiones que se formulen respecto a cada tema pericial.

II. Los peritos podrán dictaminar por separado cuando exista diversidad de opiniones entre ellos.

III. El dictamen se presentará por escrito, firmado y fechado.

NCPP - BOLIVIA: **Artículo 214°.- (Nuevo Dictamen. Ampliación).**

Cuando los dictámenes sean ambiguos, insuficientes o contradictorios, se ordenará su ampliación o la realización de una nueva pericia por los mismos peritos o por otros distintos.

NCPP - BOLIVIA: **Artículo 215°.- (Conservación De Objetos).**

I. El fiscal, juez o tribunal y los peritos procurarán que los objetos examinados sean conservados, de modo que la pericia pueda repetirse.

II. Si es necesario destruir o alterar los objetos analizados, los peritos deberán informar antes de proceder.

NCPP - BOLIVIA: Artículo 349°.- (Pericia).

I. Cuando sea posible, el juez o tribunal dispondrá que las operaciones periciales se practiquen en audiencia.

II. El juez o tribunal ordenará la lectura de las conclusiones de los dictámenes de todas las pericias practicadas en el proceso.

DOCUMENTACIÓN

La Paz, 1 de Junio de 2009

Señor:
Lic. Eufren Llanque Quispe
JEFE DE LA CARRERA DE INFORMÁTICA
Presente.-

Ref. Aval para Defensa de Tesis de Grado

De mi mayor consideración:

Tengo a bien dirigirme a su autoridad para comunicarle que luego de haber realizado el seguimiento y revisión de la Tesis de Grado "**MÉTODO INFORMÁTICO FORENSE PARA EL MANEJO ADECUADO DE LA EVIDENCIA DIGITAL Y SU ADMISIBILIDAD EN SITUACIONES JURÍDICAS EN BOLIVIA**", elaborado por la universitaria **XIMENA EUGENIA PATIÑO BUSTILLOS**. Deseo expresar mi conformidad con el contenido del mismo, otorgando mi aval para que la postulante pueda realizar la defensa pública de la mencionada Tesis de Grado, para optar al título de Licenciatura en Informática con mención en Ingeniería de Sistemas Informáticos, de acuerdo a normas y reglamentos vigentes.

Es cuanto informo y certifico para los fines consiguientes de la interesada.

Atentamente,

Msc. Lic. Mario Loayza Molina
Docente Tutor
Carrera de Informática

La Paz, 1 de Junio de 2009

Señor:
Msc. Lic. Mario Loayza Molina
DOCENTE TUTOR DE TALLER DE LICENCIATURA II
CARRERA DE INFORMÁTICA - UMSA
Presente.-

Ref. Aval para Defensa de Tesis de Grado

De mi mayor consideración:

Mediante la presente, tengo a bien dirigirme a usted para comunicarle que luego de haber realizado el seguimiento y revisión de la Tesis de Grado **"MÉTODO INFORMÁTICO FORENSE PARA EL MANEJO ADECUADO DE LA EVIDENCIA DIGITAL Y SU ADMISIBILIDAD EN SITUACIONES JURÍDICAS EN BOLIVIA"**, elaborado por la universitaria **XIMENA EUGENIA PATIÑO BUSTILLOS.** En mi calidad de Docente Revisor, deseo expresar mi conformidad con el contenido del mismo, otorgando mi aval para que la postulante pueda realizar la defensa pública de la mencionada Tesis de Grado, para optar al título de Licenciatura en Informática con mención en Ingeniería de Sistemas Informáticos, de acuerdo a normas y reglamentos vigentes.

Con éste motivo saludo a usted con las consideraciones mas distinguidas.

Atentamente,

Lic. Grover Alex Rodríguez Ramírez
Docente Revisor
Carrera de Informática