UNIVERSIDAD RAFAEL LANDÍVAR
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
LICENCIATURA EN INVESTIGACIÓN CRIMINAL Y FORENSE

"MANEJO DE LA CADENA DE CUSTODIA EN LA RECOLECCION DE EVIDENCIA DIGITAL"

TESIS DE GRADO

LUIS EDUARDO ESCOBAR DE LEÓN
CARNET 16075-12

QUETZALTENANGO, MAYO DE 2017
CAMPUS DE QUETZALTENANGO

UNIVERSIDAD RAFAEL LANDÍVAR
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
LICENCIATURA EN INVESTIGACIÓN CRIMINAL Y FORENSE

"MANEJO DE LA CADENA DE CUSTODIA EN LA RECOLECCION DE EVIDENCIA DIGITAL"

TESIS DE GRADO

TRABAJO PRESENTADO AL CONSEJO DE LA FACULTAD DE
CIENCIAS JURÍDICAS Y SOCIALES

POR
LUIS EDUARDO ESCOBAR DE LEÓN

PREVIO A CONFERÍRSELE

LICENCIADO EN INVESTIGACIÓN CRIMINAL Y FORENSE

QUETZALTENANGO, MAYO DE 2017
CAMPUS DE QUETZALTENANGO

AUTORIDADES DE LA UNIVERSIDAD RAFAEL LANDÍVAR

RECTOR:	P. MARCO TULIO MARTINEZ SALAZAR, S. J.
VICERRECTORA ACADÉMICA:	DRA. MARTA LUCRECIA MÉNDEZ GONZÁLEZ DE PENEDO
VICERRECTOR DE INVESTIGACIÓN Y PROYECCIÓN:	ING. JOSÉ JUVENTINO GÁLVEZ RUANO
VICERRECTOR DE INTEGRACIÓN UNIVERSITARIA:	P. JULIO ENRIQUE MOREIRA CHAVARRÍA, S. J.
VICERRECTOR ADMINISTRATIVO:	LIC. ARIEL RIVERA IRÍAS
SECRETARIA GENERAL:	LIC. FABIOLA DE LA LUZ PADILLA BELTRANENA DE LORENZANA

AUTORIDADES DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

DECANO:	DR. ROLANDO ESCOBAR MENALDO
VICEDECANA:	MGTR. HELENA CAROLINA MACHADO CARBALLO

NOMBRE DEL ASESOR DE TRABAJO DE GRADUACIÓN

MGTR. RAÚL ESTUARDO LÓPEZ RODRÍGUEZ

TERNA QUE PRACTICÓ LA EVALUACIÓN

LIC. FRANCISCO RUBÉN COTTÓN

AUTORIDADES DEL CAMPUS DE QUETZALTENANGO

DIRECTOR DE CAMPUS:	P. MYNOR RODOLFO PINTO SOLIS, S.J.
SUBDIRECTORA ACADÉMICA:	MGTR. NIVIA DEL ROSARIO CALDERÓN
SUBDIRECTORA DE INTEGRACIÓN UNIVERSITARIA:	MGTR. MAGALY MARIA SAENZ GUTIERREZ
SUBDIRECTOR ADMINISTRATIVO:	MGTR. ALBERTO AXT RODRÍGUEZ
SUBDIRECTOR DE GESTIÓN GENERAL:	MGTR. CÉSAR RICARDO BARRERA LÓPEZ

Raúl Estuardo López Rodríguez

Abogado y Notario

Col. No. 8,937

Quetzaltenango 22 de noviembre de 2016

Magister. Brenda Dery Muñoz Sánchez

Coordinadora Facultad de Ciencias Jurídicas y Sociales

Universidad Rafael Landivar

Campus Quetzaltenango

Atentamente me dirijo a usted, con el objeto de remitir dictamen de asesoría de tesis del alumno **LUIS EDUARDO ESCOBAR DE LEÓN**, carné No. 1607512 de la carrera de Licenciatura en Investigación Criminal y Forense. Y a al efecto rindo **DICTAMEN FAVORABLE APROBANDO** la tesis titulada: **"MANEJO DE LA CADENA DE CUSTODIA EN LA RECOLECCIÓN DE EVIDENCIA DIGITAL"**. En la cual el estudiante ha cumplido con los requisitos establecidos por las normas de la universidad y las recomendaciones dadas. Al concluir la misma se ha establecido que constituye un aporte importante en el tema del buen manejo de la evidencia digital, el cual es además un tema novedoso que genera analizar la forma correcta de recolección de evidencia de este tipo. Así mismo aporta importantes conclusiones a efecto de implementar las normas internacionales del buen manejo de la evidencia digital al ámbito guatemalteco para evitar contaminación en la misma, y de esta manera contribuir a la justicia.

Sin otro particular me suscribo atentamente.

Dr. Raúl Estuardo López Rodríguez

ASESOR

Universidad Rafael Landívar
Tradición Jesuita en Guatemala

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
No. 071463-2017

Orden de Impresión

De acuerdo a la aprobación de la Evaluación del Trabajo de Graduación en la variante Tesis de Grado del estudiante LUIS EDUARDO ESCOBAR DE LEÓN, Carnet 16075-12 en la carrera LICENCIATURA EN INVESTIGACIÓN CRIMINAL Y FORENSE, del Campus de Quetzaltenango, que consta en el Acta No. 07152-2017 de fecha 20 de febrero de 2017, se autoriza la impresión digital del trabajo titulado:

"MANEJO DE LA CADENA DE CUSTODIA EN LA RECOLECCION DE EVIDENCIA DIGITAL"

Previo a conferírsele LICENCIADO EN INVESTIGACIÓN CRIMINAL Y FORENSE.

Dado en la ciudad de Guatemala de la Asunción, a los 15 días del mes de mayo del año 2017.

MGTR. HELENA CAROLINA MACHADO CARBALLO, VICEDECANA
CIENCIAS JURÍDICAS Y SOCIALES
Universidad Rafael Landívar

Índice

Resumen

Es necesario analizar la cadena de custodia en la recolección de evidencia digital como un aspecto específico de estudio, especialmente lo referente a los instrumentos que se deben utilizar para la debida recolección de la misma.

De forma sistematizada, pertinente resulta indispensable abordar el contenido relacionado a la cadena de custodia, la evidencia, la evidencia digital y lo relativo a los sistemas informáticos para desarrollar de forma adecuada la recolección de los indicios digitales que pudieren ser objeto de prueba en un proceso penal instruido como consecuencia de la comisión de un delito que tenga como modalidad el uso de hardware y software debidamente relacionado a un sistema operativo y su plataforma.

No es un secreto que el mundo está en constante cambio y que la informática juega un papel muy importante en la actualidad debido a su convergencia con las telecomunicaciones. Así las cosas, tampoco causan sorpresa al haber nacido una nueva disciplina que se encarga de poner orden a las nuevas relaciones que han surgido con la aparición de las tecnologías de la información y las comunicaciones.

En ese sentido nos podemos dar cuenta que también ha crecido la forma de cometer delitos y ahora se están cometiendo de manera digital y es allí donde nace la necesidad de poder hacer una recolección de evidencia digital de forma adecuada para que esta no pueda ser alterada en ningún momento y poder utilizarla como elemento de prueba durante el proceso penal, existiendo una serie de herramientas adecuadas para hacerlo.

INTRODUCCIÓN

La evidencia digital es una de las figuras de la investigación criminal que en la actualidad ha planteado nuevos retos a las instituciones encargadas de la averiguación de la verdad, conjuntamente con esta se establece la cadena de custodia digital que supone nuevos retos para la identificación, recolección, preservación y resguardo de los indicios o evidencias digitales que se generan en distintos dispositivos de tecnología. Considerar el manejo de la cadena de custodia en la recolección de evidencia digital en Guatemala resulta importante para las nuevas formas de investigación, al contemplar la influencia de la tecnología en la mayoría de procesos que realiza la persona en su vida cotidiana esto mismo genera causalmente una fuente de evidencia digital en la comisión de hechos delictivos, ya sea a través de llamadas telefónicas, mensajes, fotografías, videos, audios, sistema global de posicionamiento, registros de entradas en sistemas, creación de archivos y una innumerable lista de operaciones en las que la tecnología resulta útil, representa la importancia de la evidencia digital y la cadena de custodia que recae sobre esta.

Para el efecto, la presente investigación relacionada al manejo de la cadena de custodia en la recolección de evidencia digital tiene por objeto establecer el debido manejo de la cadena de custodia, desde su inicio para preservar la evidencia digital en las investigaciones dirigidas por el Ministerio Público en recolección de evidencia en Guatemala, para lo cual el Capítulo I aborda aspectos generales relacionados a la cadena de custodia partiendo desde su definición, la forma en que esta se debe registrar y el procedimiento general aplicado a la investigación criminal tradicional, esto implica la metodología que se desarrolla partiendo del manejo de la escena del crimen, la fijación del lugar, recolección, embalaje, rotulado, envió de los indicios o evidencias, recepción, análisis y disposición final de las evidencias consideradas relevantes en la averiguación de la verdad respecto a un hecho delictivo. Por su parte el Capítulo II aborda los aspectos más importantes de la evidencia digital partiendo de la definición de la evidencia física, así como de la evidencia digital con la mera finalidad de poder establecer las diferencias más relevantes entre ambas,

continua desarrollando las características de la evidencia digital así como la clasificación considerada por diversos autores hasta adentrarse la investigación en la importancia de la evidencia digital en las nuevas fronteras de la informática forense.

En el Capítulo III de la presente investigación se desarrollan aspectos aplicados a la evidencia digital en relación a la investigación criminal, contenido que parte desde el secuestro de dispositivos de tecnología, la creación de la bitácora de hallazgos donde comienza la cadena de custodia y lo relacionado al proceso de identificación y detección de la evidencia digital así como la respectiva recuperación de archivos borrados y la consolidación de datos o información potencialmente analizable, se aborda uno de los dispositivos utilizados en Guatemala para la recuperación de información digital como lo es el UFED y la cadena de custodia en general sobre la evidencia o indicios digitales potencialmente analizables.

Por su parte el Capítulo IV titulado Manejo de la cadena de custodia en la recolección de evidencia digital aborda aspectos generales, los riesgos de la cadena de custodia digital frente a la falta de capacidad del forense o ataques externos, una breve reseña de la fundamentación legal de la cadena de custodia digital o en su defecto de la evidencia digital, los requisitos para el manejo de la cadena de custodia en la recolección de evidencia digital y aspectos muy importantes contenidos en la Norma ISO 27037 sobre la identificación, recolección, adquisición y preservación de la evidencia digital en la cual se desarrollan aspectos para el tratamiento de la evidencia digital, alcances y requisitos normalizados uniformes para el manejo de la cadena de custodia y la evidencia digital. En cuanto al Capítulo V se integra el trabajo de campo presentando los resultados obtenidos de entrevistas planteadas a los encargados de investigación criminal que tienen relación inmediata con la evidencia digital y por ende conocen asuntos metodológicos implementados en Guatemala para la averiguación de la verdad, así como de la cadena de custodia digital y su manejo adecuado.

.

CAPÍTULO I

CADENA DE CUSTODIA

El aseguramiento de la escena del crimen resulta indispensable para garantizar el resguardo de los indicios y potenciales evidencias frente a la existencia de un aparente delito, que corresponde meramente a dilucidarse en la vía penal. La cadena de custodia es fundamental en el desarrollo de la investigación y el procedimiento probatorio para el control de los elementos físicos encontrados en el lugar de los hechos. Esta es un requisito establecido para la recolección de indicios ubicados en una escena del crimen y tiene el propósito de garantizar la integridad, conservación e inalterabilidad de los elementos materiales de prueba ya sean orgánicas o inorgánicas que se identifiquen por medio de la observación dentro de la escena de un posible delito.

Asimismo, la importancia de asegurar la escena del crimen y por medio de la cadena de custodia validar por medio de esta quien diligenció la identificación de indicios dentro de la escena del crimen. Esta permite conocer en cualquier estado del proceso penal en donde se encuentra el elemento de prueba, quien lo tiene, el nombre del perito, gabinete, científico o técnico, donde se está efectuando el análisis, creando responsabilidades hacia el funcionario que participa en el desarrollo de la cadena de custodia, así como conocer los procedimientos generales y específicos. La tarea de preservar se debe llevar a cabo en tanto el personal especializado no haya comenzado el estudio del lugar, es decir, “procese los indicios o evidencias. No hay una norma que defina exactamente qué área se va a acordonar; sin embargo, en la práctica, dependerá del estudio preliminar del lugar de los hechos y/o del hallazgo. El área ideal será la que esté más cerca de donde se encuentre la mayoría de los indicios o evidencias”.[1] El aseguramiento del lugar de los hechos es la actividad que se adelanta “para garantizar el aseguramiento o protección del lugar de los hechos

[1] Iguarán Arána, Mario German. *Manual de procedimientos para cadena de custodia*. Colombia. Instituto Nacional de Medicina Legal. 2004. Pág. 23.

con ocasión de una posible conducta punible, a fin de evitar la pérdida o alteración de los elementos materia de prueba o evidencia física. Quien efectúa el aseguramiento del lugar de los hechos debe evitar el ingreso de personas no asignadas a la diligencia como periodistas, parientes, amigos, curiosos y miembros de instituciones con alto rango, entre otros".[2] Esto por medio de la observación, análisis y valoración del lugar de los hechos Corresponde a las actividades metodológicas referentes al procesamiento del lugar de los hechos para llevar a cabo una eficaz investigación, dándole aplicación a los métodos de búsqueda de los elementos materia de prueba o evidencias físicas.

1.1. Definición de cadena de custodia

Resulta indispensable abordar el contenido de la cadena de custodia y su eficacia al momento de llevar a cabo una investigación, García Garduza refiere que la cadena de custodia "se puede definir como una secuencia de actos llevados a cabo por el Perito, el agente del Ministerio Público o el Juez, mediante la cual los instrumentos del delito, las cosas objeto o producto de él, así como cualquier otra evidencia relacionada con éste, son asegurados, trasladados, analizados y almacenados para evitar que se pierdan, destruyan o alteren y así, dar validez a los medios de prueba.

La cadena de custodia debe ser observada, mantenida y documentada",[3] resulta que cada indicio tiene su forma correcta de recolección de evidencia y también su forma correcta de poder mantener su cadena de custodia, si la cadena de custodia llegara a fallar el indicio perdería toda certeza jurídica. O si la cadena de custodia fuera iniciada de una manera errónea o incorrecta, esta también quedara anulada. Otra forma de anular el indicio es en la forma en que es recolectado ya que si es recolectado de una forma incorrecta no tendría valor probatoria ante un proceso penal. La cadena de custodia es el procedimiento "de control que se aplica al indicio o evidencia material ya sea vestigio, huella, medio de comisión, objeto material o

[2] *Ibíd*. Pág. 32.
[3] Cadena de custodia. García Garduza, Ismael. *Diccionario Jurídico*. 3ª Edición. México. Editorial Porrúa. 2009. Disponibilidad y acceso: http://www.diccionariojuridico.mx/?pag=vertermi no&id=1704 fecha de consulta 01.03.2016

producto relacionado con el delito; desde su localización por parte de una autoridad, policía o agente del Ministerio Público, hasta que la autoridad competente ordene su conclusión, según se trate de la averiguación previa o el proceso penal". [4] Desde la perspectiva ministerial, la cadena de custodia es un tema fundamental en el procedimiento penal. Como bien se sabe, los indicios que se encuentran en el lugar de investigación, en la víctima o en el probable responsable, tienen la enorme posibilidad de estar íntimamente relacionados con el hecho delictivo y, por lo tanto, de proporcionarnos valiosa información al respecto. De ser así, "dichos indicios se convierten en evidencias físicas invaluables que debemos resguardar y proteger para desahogar en el proceso. Ya sea porque nos arrojen importante información durante la averiguación previa o porque puedan ser usados como prueba en juicio, los indicios y las evidencias físicas deben ser siempre cuidados por toda autoridad que tenga contacto con ellos. Es el registro fiel del curso seguido por los indicios o evidencia desde su descubrimiento por parte de una autoridad, policía o agente del Ministerio Público, hasta que la autoridad competente ordene su conclusión, según se trate de averiguación previa, carpeta de investigación o proceso penal".[5] Los indicios que se derivan de la comisión de un hecho delictivo, implica una serie de evidencias físicas de importante valor para la averiguación de la verdad, ya que son susceptibles de utilizar durante un juicio de índole penal, por ello se dice que la cadena de custodia es un registro fiel de los indicios desde su descubrimiento por la persona competente.

La cadena de custodia de la prueba, encuentra su fundamento en el debido proceso. De tal manera, que desde ese punto de vista se define como: "El procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de administrar justicia y que tiene como fin no viciar el manejo de que ellos se haga y así evitar alteraciones,

[4] Romero Guerra, Ana Pamela. *La cadena de custodia en el ámbito federal*. México. Inacipe. 2010. pág. 4.
[5] Directores generales de servicios periciales y ciencias forenses. *Protocolo de la cadena de custodia*. México. Conferencia Nacional de Procuración de Justicia. 2011. Pág. 3.

sustituciones, contaminaciones o destrucciones."[6] Asimismo, Worrall González refiere que "resulta menester asimilar que el indicio es parte fundamental no sólo de la investigación criminal, sino igualmente lo es en todo el proceso penal acusatorio, habida cuenta que será a través de éste y de su legitimación, que se logrará el convencimiento en el ánimo del juzgador, siempre y cuando, por supuesto, dicho proceso investigativo se sujete a los procedimientos ordinarios que se refieren al registro inicial de la ubicación del indicio en sí, a su detallada y precisa descripción, marcaje numerado, fijación fotográfica, embalaje y etiquetado correspondientes, así como su posterior traslado y correcto llenado de los documentos o formatos legales que amparen tales acciones, vinculándolas con las personas involucradas en ello, procedimientos que en conjunto constituyen un requisito indispensable para el debido cumplimiento de la así llamada cadena de custodia."[7] La cadena de custodia es uno de los elementos más importantes en la investigación, depende del manejo correcto que se le puede dar, ser o no aceptada en un debate ya que al ser un más uso de la cadena de custodia pone en duda su falta de certeza jurídica indicando que no se sabe si la evidencia recolectada en la escena sea exactamente el introducido en su etapa procesal en el debate como prueba.

Para Jorge Badilla la cadena de custodia se define en los siguientes términos: "Es el procedimiento de control que se aplica al indicio material relacionado con el delito, desde su localización por parte de una autoridad, hasta que ha sido valorado por los órganos de administrar justicia y deja de ser útil al proceso, y que tiene como fin no viciar el manejo de que él se haga para evitar alteraciones, daños, sustitución, contaminación, destrucción, o cualquier acción que varíe su significado original."[8] Es indispensable convalidar la eficacia de la cadena de custodia en una correcta y adecuada investigación esto como parte de la objetividad con que deben actuar los

[6] Arbulora Valverde, Arístides. *La cadena de la custodia*. Costa Rica. Editorial Marphasa. 2000. Pág. 3
[7] Worrall González, Edward C. A. *Cadena de custodia*. México. Criminalística México. 2014. Dirección de consulta: http://criminalistica.mx/areas-forenses/criminalistica/1568-cadena-de-custodia fecha de consulta: 03.02.16
[8] Badilla, Jorge. *Procesamiento de la escena del crimen*. San José, Costa Rica, Escuela Judicial, sección de capacitación organismo de investigación judicial. 1999. Pág. 23

entes encargados de la investigación, sin embargo la ausencia de la cadena de custodia representa una valoración ineficaz por parte del juzgador.

Asimismo, es importante las consideraciones de la cadena de custodia y su repercusión en el proceso penal, en el cual a partir de la identificación de objetos indiciarios, se permite generar una certeza probatoria en el juzgador para determinar la existencia o inexistencia de un hecho delictivo. Por lo tanto "siempre es necesario identificar los objetos que fueron tomados de lugar de los hechos que son a su vez motivo de la averiguación previa estos objetos o indicios le fueron posiblemente retirados al posible responsable (un arma, droga, documentos, sangre, semen, pelo, huellas latentes, así como otros elementos biológicos y materiales) y en la práctica procesal nos podemos encontrar que qué el probable responsable argumente que dichos indicios u objetos le fueron sembrados, o que estos fueron alterados o cambiados de alguna forma, es decir, qué no se encuentran en el mismo estado en que fueron hallados, o que simplemente son objetos diferentes".[9] En este sentido la cadena de custodia es el mecanismo que garantiza la autenticidad de los elementos de prueba que se aportan al proceso, es efectuado por los funcionarios y personas bajo la cual se encuentre los elementos de prueba, iniciándose con la persona que recolecta los elementos de prueba, la cual se debe de aplicar en todos los elementos probatorios los cuales deben ser descritos en el acta de la diligencia relacionando exactamente su procedencia para evitar la alteración o cambio de alguna u otra forma.

Es la cadena de custodia una de las formas mediante las cuales "el ministerio público puede identificar los objetos o indicios obtenidos en el lugar de los hechos es la demostración de que se ha cumplido una estructura cadena de custodia. Un indicio, antes de ser presentado ante un juez penal, debe haber recorrido diferentes etapas, de tal suerte, que él mismo pueda ser considerado como prueba durante el proceso penal. El indicio debe ser sujeto a determinados experimentos y confrontaciones

[9] Mora Izquierdo Ricardo y María Dolores Sánchez Prada. *La evidencia Física y la Cadena de Custodia dentro del procedimiento penal acusatorio.* Bogotá, Colombia. Editores Gráficos. 2007. pág. 567.

antes de adquirir la calidad de prueba. Antes de que un indicio puede adquirir el carácter de prueba en proceso penal, se deben hacer los siguientes cuestionamientos: ¿Cómo se puede saber que un determinado indicio pertenece a un caso particular, y no a otro similar? ¿Cómo tener la seguridad de que un determinado indicio no ha sido manipulado con el propósito de obtener un resultado favorable o adverso? La objetividad en el manejo de los indicios es vital para que estos puedan adquirir la calidad de prueba durante el proceso penal y mediante ellos o ellas dictar sentencia objetiva e imparcial".[10] La objetividad de la cadena de custodia es un principio que se encuentra relacionado íntimamente a la actividad investigativa del Ministerio Público y que se encuentra establecido en la Ley Orgánica del Ministerio Público en el artículo uno de forma general y que trae consigo un revestimiento de cualquier actividad relacionada a la investigación y la cadena de custodia de la manera siguiente: "El Ministerio Público es una institución con funciones autónomas, promueve la persecución penal y dirige la investigación de los delitos de acción pública; además velar por el estricto cumplimiento de las leyes del país. En el ejercicio de esa función, el Ministerio Público perseguirá la realización de la justicia, y actuará con objetividad, imparcialidad y con apego al principio de legalidad, en los términos que la ley establece". Este mismo precepto se relaciona íntimamente con el artículo 108 del Código Procesal Penal el cual refiere que "En el ejercicio de su función, el Ministerio Público adecuará sus actos a un criterio objetivo, velando por la correcta aplicación de la ley penal", la objetividad se refiere íntimamente a la imparcialidad con la que debe actuar el Ministerio Público más allá de recurrir a una actitud meramente acusatoria, velando por la preservación de la Justicia dentro del proceso penal guatemalteco.

Para Ricardo Mora izquierdo y María Dolores Sánchez Prada, la cadena de custodia es "el sistema de aseguramiento de la evidencia física compuesto por personas Como normas, procedimiento, información, contenedores y lugares, que al avalar el cumplimiento del principio de mismidad, garantiza la autenticidad de la evidencia que

[10] *Loc. cit.*

se recolecta y analiza, y que se exhibe en la audiencia pública del juicio oral".[11] Así mismo para Bernal Arévalo Benjamín citado por Mora y Sánchez, la cadena de custodia es un "sistema de seguridad que garantiza que la evidencia que llega al laboratorio para análisis es la misma que está en la escena explorada; igualmente, qué es la misma evidencia que una vez analizada, se devuelve al solicitante y que se lleva a la audiencia pública del juicio, acompañada del dictamen pericial respectivo".[12] La cadena de custodia es un procedimiento establecido por la normativa jurídica, que tiene el propósito de garantizar la integridad, conservación he inalterabilidad de los elementos materiales de prueba como documentos, muestras orgánicas e inorgánicas, armas de fuego, proyectiles, armas blancas, estupefacientes y sus diversidades entregándolos a los laboratorios criminalísticas o forenses.

Por lo tanto la cadena de custodia es un procedimiento de control "que se aplica al indicio, que bien puede ser una mancha, una huella, un medio de comisión, Objeto material, o bien el producto de un delito. Desde su localización por parte de la autoridad hasta que la autoridad competente ordene su conclusión, el propósito de este procedimiento consiste en que dichos elementos materiales (indicios) no sean alterados, modificados, cambiados, destruidos o que desaparezcan".[13] Para realizar una efectiva preservación del lugar de los hechos se deberán emplear las técnicas adecuadas de acordonamiento, "lo cual dependerá de cada caso en particular, y de que el área sea abierta, cerrada o mixta. La acción de preservar el lugar de los hechos y/o del hallazgo, a cargo del personal de la policía, no sólo consiste en acordonar, sino en impedir que:

- Otras personas deambulen innecesariamente por el lugar.
- Se manipulen objetos que pudieran servir de indicios o evidencias.
- Alguien toque los cuerpos o restos humanos.
- Se contaminen objetos en que pudieran encontrarse huellas dactilares.
- Se toquen objetos sin el permiso del personal que resguarda el lugar.

[11] *Ibíd.* Pág. 511
[12] *Loc. cit.*
[13] *Loc. cit.*

- Se desechen objetos que pudieran tener relación con el hecho".[14]

En este sentido, la preservación de los indicios u objetos que sean parte de la escena de un delito deben seguir ciertos parámetros, los elementos recolectados deberán se acompañados por la cadena de custodia a través del procedimiento judicial, los elementos probatorios deben ser debidamente embalados según el protocolo de diferentes laboratorios. Todo funcionario o perito deberá de detallar en el dictamen los procedimientos que se aplicaron al elemento de prueba, por lo que en el formato de cadena no se admiten borrones, tachas, espacios líneas en blanco, tintas de diferentes colores, ni adiciones en la copia. El control de la cadena se seguirá ya en el interior de los laboratorios correspondientes.

La recolección, embalaje y rotulado de los elementos materia de prueba o evidencias son actividades implementadas para ser enviados a los correspondientes laboratorios o bodegas de evidencias, en condiciones de preservación y seguridad que garanticen la integridad, continuidad, autenticidad, identidad y registro, de acuerdo a su clase y naturaleza. El desconocimiento de la cadena de custodia no exime de responsabilidad al miembro de cualquier institución que los omita en determinado momento. El funcionario, al momento de recolectar los elementos de prueba debe dejar constancia en el acta de la diligencia correspondiente sobre la aplicación de cadena de custodia.

1.2. Registro de la cadena de custodia

El registro de la cadena de custodia consiste en "el formato o formatos dentro de los cuales deberán anotarse los nombres y firmas de los servidores públicos que de manera sucesiva intervengan en la cadena de custodia, desde que se hallan los indicios hasta el final del proceso. Además se debe anotar la fecha y hora de entrega y recepción del indicio, la descripción de los objetos o indicios, sus características físicas, color, peso, etcétera, el lugar de los hechos o del hallazgo Y todos los datos

[14] Directores Generales de Servicios Periciales y Ciencias Forenses. *Óp. cit.* Pág. 20.

que se consideren relevantes para la averiguación previa".[15] Pese a la existencia de formatos para el registro de la cadena de custodia, en ocasiones no se cuenta con los mismos, circunstancia que debe ser tomada como irrelevante para la recolección de los objetos o indicios en el lugar de los hechos presuntamente delictuosos. La policía, así como los peritos, deben estar capacitados para improvisar de forma inteligente, de tal suerte que se evite la alteración de lugar de los hechos y la bebida recolección de los indicios. La información que debe contener el registro de la cadena de custodia, de acuerdo con la legislación es la siguiente.

1. número de averiguación previa.
2. Unidad administrativa responsable.
3. Ubicación e identificación del lugar con croquis.
4. Información relativa a las víctimas, Detenidos, testigos o cualquiera que se recarguen en el lugar de los hechos o del hallazgo.
5. Nombre completo, cargo y firma de los servidores públicos que han intervenido en la preservación de lugar de los hechos o del hallazgo.
6. Fecha y hora".[16]

Los peritos deberán detallar el informe correspondiente de las acciones que se han adoptado para el procedimiento de los indicios, además de anotar las medidas que se han implementado para garantizar la integridad de estas, así como el nombre y firma de las personas que intervinieron en las referencias referidas acciones. Esto permite asegurar la pureza de lo recabado en la escena criminal y sobre todo proporciona una certeza intrínseca que refiere que esto podrá ser útil durante el desarrollo del proceso penal en relación al crimen investigado.

1.3. Procedimiento de la cadena de custodia

La Cadena de Custodia representa una serie de "actividades eslabonadas, encaminadas a la correcta y adecuada preservación de los indicios o evidencia

[15] Mora Izquierdo Ricardo y María Dolores Sánchez Prada. *Óp. cit.* Pág. 518.
[16] *Loc. cit.*

material desde su descubrimiento en lugar de hechos por parte de una autoridad, hasta que autoridad competente ordene su conclusión, según se trate de averiguación previa, carpeta de investigación o el proceso penal".[17] La preservación de los indicios o evidencia en la escena del crimen es el fundamento de la existencia de la cadena de custodia, siendo esta una institución del sistema acusatorio en la cual el Ministerio Público por medio de su departamento forense tiene a su cargo la investigación de los hechos acaecidos, la observancia del protocolo de la cadena de custodia es importante para la conservación de la evidencia que es susceptible de integrarse a la administración de justicia. En consecuencia si no es posible garantizar la autenticidad de la evidencia esta pierde su valor probatorio, siendo inútil su utilización dentro del proceso penal para las partes, cualquier procedimiento policiaco, investigativo, judicial y pericial, que se relacione de alguna manera con indicio físico o biológico, debe garantizar el respeto a la cadena de custodia y el cumplimiento de las normas reglamentarias y los postulados científicos que la orientan.

Los Directores Generales de Servicios Periciales y Ciencias Forenses de México en la Conferencia Nacional de Procuración de Justicia realizada en el año 2011 refieren que "la Cadena de Custodia se divide en 6 grandes etapas:

1. Protección y Preservación de lugar de los hechos y/o del hallazgo.
2. Procesamiento de los Indicios o Evidencias.
3. Entrega al Ministerio Público de los Indicios o Evidencias e Integración del Registro a la Averiguación Previa o Carpeta de Investigación.
4. Manejo de los Indicios o Evidencias en los Laboratorios.
5. Manejo de los Indicios o Evidencias en la Bodega de Evidencias.
6. Manejo de las Evidencias Provenientes de Entidades Prestadoras de Servicios de Salud Pública o Privada".[18]

[17] Directores Generales de Servicios Periciales y Ciencias Forenses. *Óp. cit.* pág. 5.
[18] *Ibíd*. Pág. 5.

Estas seis etapas son fundamentales para el desarrollo pleno de la cadena de custodia, en primer lugar la protección y preservación del lugar de los hechos debiéndose adoptar las medidas necesarias para evitar alterar la escena material que brinda consecuentemente indicios sobre el hecho acaecido, en un caso específico la policía al ser el ente primero en apersonarse debe tener capacitación suficiente para evitar alterar irreversiblemente los indicios y posibles evidencia, así como impedir el ingreso de personas no idóneas a la escena del crimen que pudieran modificar o suprimir posible evidencia, para esto se utiliza el acordonamiento el cual es un mecanismo que delimita la escena del crimen y es referencia a que se prohíbe el ingreso de particulares o sujetos no autorizados a un lugar en específico sometido a investigación. El fiscal encargado del caso, es el responsable de verificar el cumplimiento del inicio de la cadena de custodia y el envío a donde corresponde de los distintos indicios o evidencias recolectados en la escena del crimen o lugar del hallazgo.

El técnico embalador es el responsable directo del resguardo físico adecuado de los indicios recolectados, embalando estos acorde a la particularidad del indicio, para garantizar su seguridad, inalterabilidad y evitar su contaminación, deterioro o destrucción, o que los mismos se puedan derramar, dañar o contaminar a quienes lo manipulen, así como de su inmediato envío a donde corresponda, conforme las instrucciones del fiscal a cargo. El procesamiento de los indicios o evidencias es una compleja actividad ya que se vale de la observación para identificarlos, a partir del razonamiento lógico y estructural que permite inferir cuales pudieron haber sido los elementos que son propios de la escena del crimen, a partir de la identificación de estos resulta indispensable su individualización, identificación y sobre todo su recolección que debe observar los parámetros estipulados en los manuales respectivos. Previo a la entrega de los indicios o evidencias por parte del auxiliar fiscal que asiste la escena del crimen este debe de sellarlas en sus respectivos recipientes e identificarlas y sobre todo colocar su nombre conjuntamente con los demás requisitos. Las demás etapas son propias de la investigación que se desarrolla con la intención de manejar, estudiar y justificar la razón del porque para el

ente investigador los indicios recolectados son parte fundamental de la averiguación de la verdad para lo que la cadena de custodia permite identificar quienes han manejado la evidencia y sobre todo para generar la certeza en el juzgador sobre la idoneidad de la prueba aportada. Desde el momento que se inicia el procesamiento de un indicio y su recolección por parte del Ministerio Público, Policía Nacional Civil y todos los agentes involucrados en dicho procesamiento, la custodia de los indicios deberá ser llevada estrictamente para que en el momento de hacer entrega de los indicios a las distintas oficinas, se tenga un orden lógico y enmarcado en el ámbito jurídico y así validar su manejo. Para el efecto el coordinador del grupo de turno, deberá supervisar el cumplimiento de los procedimientos de fijación, registro y completar los documentos específicos para el efecto. El manual de procedimientos para cadena de custodia de la Fiscalía General de la Nación del Estado de Colombia establece una serie de pasos que son parte de una cadena de custodia adecuada, con el fin de preservar de la mejor manera la escena del crimen y los indicios que de ella nacen, estableciendo los siguientes:

1.3.1. Manejo del lugar de los hechos:

Se considera que es la "actividad que se adelanta para garantizar el aseguramiento o protección del lugar de los hechos con ocasión de una posible conducta punible, a fin de evitar la pérdida o alteración de los elementos materia de prueba o evidencia física. Aplica a la primera autoridad que haga presencia en el lugar, personas y lugares relacionados. Inicia con la primera autoridad que llega al lugar de los hechos, una vez se haya verificado y confirmado la noticia criminal y finaliza con la entrega del lugar de los hechos al servidor designado o encargado para el manejo de la diligencia o autoridad competente".[19] Es recomendable según la Fiscalía General de la Nación del Estado de Colombia que el manejo adecuado del lugar de la escena del crimen permite realizar una investigación eficaz, en la cual es necesario adelantar la preservación y aseguramiento del lugar conjuntamente con su entorno para evitar la pérdida o alteración de elementos que eventualmente puedan constituir prueba; por

[19] Fiscalía General de la Nación. *Manual de procedimientos para cadena de custodia*. Colombia. 2004. Pág. 32

lo general esta aplica a la primera autoridad que haga presencia en el lugar, personas y entorno relacionado a fin de garantizar la protección de cualquier elemento indiciario que se relacione a la naturaleza y forma del delito. Estas actividades deben ser metodológicas y se deben aplicar especialmente a la búsqueda de los elementos que posiblemente pueden constituir prueba al instruir el proceso penal o en defecto consideradas evidencias físicas.

1.3.2. Fijación del lugar de los hechos

Como según paso o etapa para una adecuada cadena de custodia, se debe fijar el lugar de los hechos. Esto implica básicamente realizar una descripción detallada del lugar en el que se cometió un hecho o acto criminal, su entorno y elementos que configuran la escena del crimen; estos elementos indiciarios posteriormente pueden ser materia de prueba en la correspondiente imputación penal por lo que la recolección de posibles evidencias se debe realizar utilizando técnicas preestablecidas, especializadas y legalmente aceptadas. La fijación del lugar de los hechos desde su aspecto descriptivo implica a su vez la identificación de todos los elementos físicos o tangibles que configuran la escena del crimen, por lo que la metodología de la observación es indispensable, ya que los detalles son una parte sustancial en la investigación criminal a fin de alcanzar de forma objetiva una adecuada determinación de cómo se cometió el crimen, cuándo en una esfera de tiempo o rangos temporales, el por qué como un elemento subjetivo y que se utilizó para ejecutar el crimen.

1.3.3. Recolección, embalaje y rotulado de los elementos materia de prueba o evidencias

Como tercer paso se procede a la recolección, embalaje y rotulado de los elementos considerados como indicios o evidencias que han sido identificados en la escena del crimen, para su efecto son “actividades que se desarrollan en forma adecuada, para ser enviados a los correspondientes laboratorios o bodegas de evidencias, en condiciones de preservación y seguridad que garanticen la integridad, continuidad,

autenticidad, identidad y registro, de acuerdo a su clase y naturaleza".[20] Es indispensable que de forma adecuada y cuidadosa se realice la recolección, embalaje y rotulado de todos aquellos elementos que se han identificado dentro de la escena del crimen que pueden aportar una explicación en relación al delito según su naturaleza, estas actividades son fundamentales para su posterior remisión a los laboratorios o bodegas de evidencia tal como lo señala el autor, por lo que parte de la cadena de custodia implica la preservación y seguridad de dichos elementos para guardar la integridad, autenticidad y especialmente la identidad de cada objeto que se ha descubierto en la escena del crimen.

1.3.4. Envío de los elementos materia de prueba o evidencias al almacén transitorio

Se le denomina envió de los elementos materia de prueba o evidencias al almacén transitorio previo a su presentación en los tribunales para su respectiva valoración, a "las actividades desplegadas por la Policía o quien haga sus veces para disponer el almacenamiento transitorio de las sedes administrativas mientras se envía al laboratorio autorizado o al almacén general de evidencias".[21] Estas sedes de carácter administrativo que están subordinadas a la institución encargada de la investigación criminal tienen como función el resguardo adecuado de las evidencias recolectadas, El traslado o transporte de los indicios o evidencias debe ser cuidadoso y meticuloso, tomando en consideración las condiciones climatológicas, la temperatura del transporte, la presión y el movimiento, así como la duración del mismo, ya que pueden causar la destrucción del indicio o evidencia. La instrucción 104, 105, 106, 107 del Manual de normas y procedimientos para el procesamiento de la escena del crimen del Ministerio Público de Guatemala refiere respecto al traslado de las evidencias lo siguiente: "el técnico embalador remite los indicios al laboratorio, a través del formato de la DICRI número URE-02-Solicitud de análisis, entrega de indicios, cadena de custodia en el que consignará los datos del caso, indicando el tipo de análisis solicitado, conforme instrucciones del fiscal a cargo… El técnico

[20] *Ibíd.* Pág. 50
[21] *Ibíd.* Pág. 58

embalador entrega los indicios al lugar a donde corresponda, de no requerir ningún análisis, los indicios deberán remitirse a través del formulario URE-02.

1. En la ciudad Capital, se entregan directamente al Almacén Central de Evidencias.
2. en los demás municipios y departamento, se entregan a la bodega de evidencias de la fiscalía municipal o distrital, para su posterior traslado, en condiciones de seguridad, al Almacén Central de Evidencias en la Ciudad Capital".

Los formatos tienen incluido el registro de cadena de custodia y deben ser firmados y sellados por el embalador y el Fiscal a cargo.

El Fiscal como responsable legal de la custodia de los indicios, una vez embalados es quien ordena hacia donde se remiten:

a. "Dinero, valores: a la bóveda de valores del Ministerio Público; de conformidad con el monto incautado, coordinará su traslado con el Encargado del Almacén Central de Evidencias y el Jefe del Departamento de Seguridad del Ministerio Público, en los términos que establece el normativo para la guarda, custodia y conservación de evidencias en la bóveda del Ministerio Público, aprobado por acuerdo 37-2008 y la instrucción 011-2008 de fecha 28 de agosto de 2008, emitida por el jefe administrativo.
b. Drogas, fármacos o estupefacientes, precursores o similares: a la Subdirección General de Análisis e Información Antinarcótica -SDGAIA- a través de la Policía Nacional Civil.
c. Vehículos: a la bodega de inspección vehicular del Ministerio Público o en su defecto, a los predios de la PNC.
d. Armas de fuego: Deberán ser remitidas al INACIF
e. Los indicios que requiera otro tipo de análisis especial se remiten a donde corresponda según su naturaleza".

Es en el Manual de normas y procedimientos para el procesamiento de la escena del crimen del Ministerio Público de Guatemala en donde se establecen los almacenes transitorios de las evidencias recolectadas en la escena del crimen, siendo estos

adaptados a nivel de infraestructura y con las condiciones ambientales adecuadas para la preservación de los elementos recolectados en la escena del delito. El fin de clasificar de forma adecuada los almacenes temporales se debe a que la disponibilidad, ubicación e identificación de los indicios, evidencias y pruebas sea inmediata ya que las condiciones de un proceso penal pueden variar repentinamente, por lo que la evidencia debe estar inmediata a los interesados para su inspección y valoración en un juicio debidamente instruido.

1.3.5. Recepción y análisis de los elementos materia de prueba o evidencias en el laboratorio autorizado.

Es parte del procedimiento de la cadena de custodia la recepción y análisis de los elementos recolectados en la escena del crimen, para el análisis se entiende como "las actividades desplegadas por los Laboratorios Autorizados para la recepción de los elementos materia de prueba o evidencias físicas con el fin de realizar los estudios o análisis solicitados por la autoridad judicial".[22] Es en este punto donde todos aquellos indicios y objetos recolectados en la escena del crimen se someten a estudios especializados y análisis requeridos por los jueces que tienen conocimiento de la causa penal, la labor que realizan los peritos en base a los conocimientos profesionales y específicos en cierta materia ponen en marcha la objetividad del Ministerio Público al convalidar la hipótesis circunstancial que se maneja en la imputación o excluir elementos ajenos al crimen, por lo que indudablemente es uno de los pasos más importantes en la investigación forense y criminal ya que es en este punto donde es posible concluir por parte del investigador de forma aproximada que es lo que realmente sucedió.

1.3.6. Disposición final de los elementos materia de prueba o evidencia

El objeto de la cadena de custodia se materializa con la disposición final de los elementos materia de prueba o evidencias físicas recolectadas en la escena del crimen, esto implica su destino final el cual corresponde a la presentación para su valoración a la autoridad judicial competente que tiene conocimiento del proceso

[22] *Ibíd.* Pág. 68

penal instruido debidamente a razón de la comisión de un delito en específico, estos tribunales pueden ser especializados o de mayor riesgo por la naturaleza del delito, pero la cadena de custodia cumple el mismo fin como parte del resguardo y aseguramiento de la evidencia recolectada en la escena del crimen. Es en este punto donde la cadena de custodia de las evidencias se transmite al juzgador para que este pueda apreciarla en base a la inmediación y valorarla en su conjunto para emitir posteriormente una resolución motivada y razonada.

1.4. Requisitos respecto a la información de la cadena de custodia

Cada persona que participa en el procesamiento de la escena del crimen y en la investigación operativa es responsable del contenido, elaboración y entrega oportuna del informe correspondiente.

a. **"**Informe de investigación operativa (preliminar): serán entregado, en la reunión de evaluación de turno de setenta y dos horas directamente al fiscala cargo, con copia para el archivo de la DICRI a través del coordinador de grupo de investigación operativa.

b. Informe del procesamiento de la escena del crimen: el coordinador del grupo que proceso la escena del crimen y recolectó los indicios o realizó el apoyo a la fiscalía, será el responsable de la recopilación de cada parte del informe, su integración y entrega al sub coordinador de grupos de procesamiento de la escena del crimen y recolección de indicios, o de la persona designada para efectos de su revisión y verificación del cumplimiento de las normas establecidas y envío a donde corresponda".[23]

La cadena de custodia debe ser la constante en todos los procedimientos que se usan en la técnica criminalística, en la medicina legal, en todas las ciencias forenses y no únicamente unas reglas que se utilizan al explorar la escena de los homicidios, como se piensa usualmente. En todo caso, las escenas del delito son tan diversas

[23] Ministerio Público. *Manual de normas y procedimientos para el procesamiento de la escena del crimen*. Guatemala. Acuerdo 166-2013.

como la misma tipicidad del código penal lo permite. La Fiscalía General de la Nación de Colombia refiere que la documentación del sistema de cadena de custodia resulta importante especialmente en los aspectos descriptivos ya que "es la actividad por la cual se hace constar las particularidades de los elementos materia de prueba, de los custodios, el lugar, sitio exacto, fecha y hora de los traspasos y traslados del elemento materia de prueba o evidencia física, entre otros; mediante el diligenciamiento de los formatos de entrega del lugar de los hechos, rótulo y de registro de cadena de custodia, para efectos de demostrar la identificación del elemento y la continuidad de la cadena de custodia".[24] La documentación de la cadena de custodia cumple una función objetiva que permite evidenciar la continuidad de la cadena de custodia y a su vez identifica de forma pertinente el elemento considerado evidencia o indicio, esto incluye especialmente a los individuos que han intervenido en la escena del crimen y las particularidades de cada evidencia considerando el sitio exacto, fecha y hora de traslados de la evidencia física.

La Cadena de Custodia de los indicios o evidencias, debe nacer a la luz del proceso penal en sus diferentes fases y quedar establecidas las pautas que deberán seguir las personas que reglamenten, desarrollen, apliquen y controlen la cadena de custodia. Los Directores Generales de Servicios Periciales y Ciencias Forenses indican que "La información mínima que se debe disponer en la Cadena de Custodia, para un caso específico, es la siguiente:

a. "Una hoja de ruta, en donde se anoten los datos principales sobre descripción del indicio, fechas, horas, responsable del indicio, identificaciones, cargos y firmas de quien recibe y de quien entrega;
b. Recibos personales que guarda cada responsable del indicio y en la que aparecen los datos similares a los de la hoja de ruta;
c. Rótulos que van adheridos o pegados a los envases o embalajes de los indicios, por ejemplo a las bolsas plásticas, sobres de papel, sobres de manila, frascos, cajas de cartón, etc.;

[24] Fiscalía General de la Nación. *Óp. cit*. Colombia. 2004. Pág. 118.

d. Etiquetas que tienen la misma información que los rótulos, pero van atadas con una cuerda a las bolsas de papel kraft, frascos, cajas de cartón o sacos de fibra;
e. Libros de registro de entradas y salidas, o cualquier otro sistema informático que se debe llevar en los laboratorios de análisis, en las oficinas del Ministerio Público y en Bodega.
f. Registro de las Condiciones de Almacenamiento (temperatura, humedad, etc.). Todos los formatos a utilizar en la Cadena de Custodia deben estar reimpresos y estar disponibles para los investigadores y Ministerios Públicos que atiendan un caso".[25]

El técnico embalador busca los indicios aplicando el método establecido en el plan de procesamiento respectivo definido por el coordinador y fiscal a cargo, procediendo a su fijación. Por lo que debe verificar que el indicio haya sido documentado a través de fotografía y video-filmación. Conjuntamente con esto marca con dos iniciales cada indicio, en un lugar que no altere su forma ni su contenido, cuando sea posible hacerlo, acción que se indicará en el informe correspondiente. Debe ser indispensable la documentación en el formato URE 02 y URE 05, cada indicio según el número con que se fijó y embala, individualmente por separado en forma adecuada a su tamaño y naturaleza, cuidando además que no se dañen elementos que serán objeto de análisis en el laboratorio, como tampoco que haya contaminación o transferencia entre los mismos. Asimismo, describe en forma precisa el indicio; descripción que se anota en el empaque del embalaje y en la cadena de custodia. En el empaque deberá anotarse la información siguiente: número de caso Ministerio Público, número de informe, fecha, hora, Agencia Fiscal que corresponde, motivo de la diligencia, nombre de la víctima y del imputado cuando sea el caso, lugar donde se embala el indicio, número de indicio o evidencia, descripción, nombre y firma de quien embala, nombre y firma del fiscal a cargo. Por ultimo Firma y sella la cadena de custodia, solicita firma y sello del fiscal a cargo".[26] La cadena de custodia debe observar formalidades de ley que se encuentran

[25] Directores Generales de Servicios Periciales y Ciencias Forenses. *Óp. cit.* Pág. 11.
[26] Ministerio Público. *Manual de normas y procedimientos para el procesamiento de la escena del crimen*. Guatemala. Acuerdo 166-2013.

establecidas en manual de normas y procedimientos para el procesamiento de la escena del crimen del Ministerio Público de Guatemala, en este sentido más allá de que las personas que intervienen en el diligenciamiento de la escena del crimen y la identificación conjuntamente con la recolección de los indicios deben ser autorizadas e idóneas para el desarrollo de estas diligencias de investigación deben observarse los aspectos técnicos, procedimentales y formales de la cadena de custodia para asegurar su fiabilidad al momento de integrarse al proceso penal guatemalteco instruido en contra del supuesto responsable de un delito.

CAPÍTULO II

EVIDENCIA DIGITAL

El siglo XXI está lleno de innovaciones tecnológicas, a primera vista la sociedad puede parecer bastante avanzada. En realidad, sólo es una aproximación del futuro próximo en el que la tecnología y los dispositivos innovadores forman parte de la vida constante de las personas, la industrialización y procesos en los que influye la tecnología son cada vez más constantes creando una relación íntima entre esta y el ser humano. Sin duda alguna, el mundo digital es influyente en las sociedades actuales por lo que la identidad, privacidad y quehaceres forman parte de las distintas bases de datos conformadas por extensos servidores asentados en distintos países que conforman un mundo digital, en el que la información es redireccionada según las necesidades del cliente, usuario o administrador de un dispositivo digital, estas transferencias o flujos de información crean una serie extensa e ilimitada de rastros que consecuentemente pueden evidenciar la comisión de un hecho delictivo, creando un vínculo estrecho entre la rama del derecho penal y la unificación de sistemas binarios que permiten la digitación, navegación, almacenamiento, creación, modificación o supresión de información digital según las necesidades del individuo.

Un juicio penal es un procedimiento contradictorio en el que tanto la fiscalía como la defensa prueban sus casos mediante la presentación de pruebas. La evidencia puede ser un testimonio de una persona que tiene conocimiento personal de hechos relacionados con el delito, o puede ser una evidencia física, que es un elemento tangible, como un arma homicida, un registro de servidor de seguridad o un disco duro que contiene datos. Para su efecto resulta importante abordar de forma preliminar la evidencia física ya que a partir de los aspectos más relevantes de esta es posible crear una adecuada definición de la evidencia digital e identificar los elementos que caracterizan todos aquellos indicios o evidencias digitales que por su naturaleza, sean indispensables para la comisión de un delito.

2.1. Definición de evidencia física

El objeto de la investigación criminal, es la recolección de indicios o evidencias que permitan generar una certeza jurídica y verídica respecto al acaecimiento de un hecho delictivo, los elementos que intervinieron y las consecuencias materiales que representan el agravio directo sobre un bien jurídico tutelado por la Constitución Política de la República de Guatemala y otras leyes de carácter ordinario, en este sentido para Laura Casado evidencia es la "certeza clara, manifiesta y tan perceptible que nadie racionalmente puede dudar de ello".[27] El verbo evidencia hace referencia a una certeza innegable para el razonamiento de quien valora, en este caso la evidencia adquiere diversas formas. Dentro de la investigación la evidencia se le puede denominar "criminal", ya que de un acto tipificado por normas prohibitivas se deriva la necesidad de la búsqueda de la verdad respecto a las condiciones imputadas a un sujeto.

El argentino Carlos Guzmán refiere que cuando "se exploran los objetivos principales de la investigación en el escenario del delito, las áreas de importancia pueden resumirse de la siguiente manera: colección o acopio de la evidencia física, reconstrucción del hecho, identificación y eslabonamiento del sujeto con el escenario del suceso y establecimiento de la causa probable de arresto. En la persecución de tales objetivos, el área policial encargada de la colección, preservación y documentación de la evidencia, así como de la investigación en el lugar del hecho, ha descubierto en ello un arte. Con el propósito de desarrollar una comprensión del rol prominente que juega la evidencia física en el entorno legal contemporáneo, una evolución perspectiva es una necesidad. Básicamente hay tres caminos principales, disponibles para coadyuvar en la solución de un hecho: confesión del sujeto, manifestaciones de una víctima o testigos, y la información obtenida a través de la evidencia física".[28] Para que la evidencia pueda ser tratada por el técnico y personal a cargo de la investigación se le debe concebir a esta pieza importante del proceso penal como una evidencia física criminal que genera una plena certeza en el

[27] Evidencia. Casado, Laura. *Diccionario de Derecho*. Argentina. Ediciones Valleta. 2008. Pág. 165.
[28] Guzmán, Carlos. *Manual de Criminalística*. Buenos Aires, Argentina. Ediciones de la Roca. 2000. Pág. 39, 40.

juzgador, la evidencia material genera una prueba fiel a diferencia de los testigos quienes pueden ser cuestionados en la información que aportan y contravenidos del razonamiento de la evidencia física criminal. Por lo que la evidencia física es todo elemento tangible que permite centrar una observación y es útil para apoyar o confrontar una hipótesis.

La evidencia física, finalmente, es normalmente inanimada y provee realidades o hechos imparciales; se ha dicho "repetidas veces que constituye el testigo mudo del evento. Si se la utiliza con eficacia puede superar una serie de afirmaciones conflictivas y confusas ofrecidas por testigos que observaron el mismo incidente al mismo tiempo. El suministro potencial que brinda la evidencia física guarda relación directa con la actitud de aquéllos encargados de obtenerla. La actitud más benéfica y constructiva es aquella que enfatiza que su detección siempre será lograda cuando el tiempo y el esfuerzo sean utilizados de una manera metódica. Nada estará excluido de consideración y la búsqueda no terminará hasta que se esté completamente seguro de que todas las posibilidades han sido exploradas. De igual valor al desarrollo de las adecuadas actitudes será el control de la emoción. Las influencias emocionales que puedan existir deben ser reconocidas y controladas, en orden a que la búsqueda sea organizada y metódica".[29] La evidencia física cumple un papel importante en la averiguación de la verdad ya que, como bien lo indica Guzmán es el testigo mudo de un determinado evento, en el cual cuando esta resulta eficaz supera las afirmaciones confusas de los testigos que observaron el mismo evento al mismo tiempo pero que se condiciona por circunstancias cognitivas y propias del individuo respecto a la identificación de patrones o características que son distintas en cada evento criminal. Estas evidencias físicas que son recolectadas durante las diligencias del Ministerio Público se materializan a final de su tratamiento en pruebas que son naturales al proceso penal, donde se practica la actividad probatoria bajo los principios de inmediación y libre apreciación del juzgador; asimismo la contradicción y oralidad permiten un diligenciamiento práctico y sobre todo equitativo para las partes que intervienen. En una definición que reúne los

[29] *Loc. cit.*

criterios fundamentales de la prueba y la materialización de la evidencia en el proceso penal, el tratadista Manuel Ossorio indica que prueba es el "conjunto de actuaciones que dentro de un juicio, cualquiera que sea su índole, se encaminan a demostrar la verdad o la falsedad de los hechos aducidos por cada una de las partes, en defensa de sus respectivas pretensiones litigiosas… prueba es toda razón o argumento para demostrar la verdad o la falsedad en cualquier esfera y asunto"".[30] La prueba es un conjunto de evidencias e indicios que encamina a demostrar la verdad o falsedad de un hecho criminal, por parte del juzgador esta debe ser apreciada en observancia de la inmediación y sobre todo debe ser valorada en su conjunto por medio de la sana critica razonada, para lo cual el argumento de la importancia de la evidencia recae en la esencia de veracidad o contradicción de las afirmaciones que son objeto de valoración dentro de un proceso penal instruido como consecuencia de un delito.

El fundamento e importancia de la evidencia recae en la manifestación de la certeza que esta puede proveer en su momento procesal oportuno, y por medio del cual el Ministerio Público puede convalidar su hipótesis acusatoria o simplemente en observancia del principio de objetividad desechar afirmaciones que sean falsas al momento de la imputación de un hecho delictivo, en este sentido resulta importante comprender que la evidencia atraviesa una evolución o transformación material que se representa por medio de la prueba válidamente admitida en el proceso penal guatemalteco, valiéndose de las técnicas de litigio por parte del Ministerio Público. Por lo que la manifestación de la justicia derivada de la comisión de un hecho delictivo crea de forma oportuna la validez de la investigación forense, con un objetivo específico que es la búsqueda de la verdad a través de prácticas y conocimientos especializados que permiten el estudio de la escena del crimen desde diferentes perspectivas.

[30] Ossorio, Manuel. *Óp. cit.* Pág. 791.

2.2. Definición de evidencia digital

La evidencia digital reúne requisitos similares a la evidencia física, aunque su forma y tangibilidad varíen de forma puntual. La relación causal entre la innovación tecnológica y su influencia en la vida del ser humano denotan las circunstancias de la utilidad de las herramientas o dispositivos digitales para cualquier actividad que se realice en la actualidad. Desde redactar un documento digital con fines personales, hasta el desarrollo de software avanzado para industrializar procesos de trabajo o de producción, esto enmarca el ámbito de aplicación de la tecnología y sus dispositivos en la vida del ser humano en el presente. Por lo que es indispensable que al abordar el contenido de la evidencia digital se contenga el potencial de la mente abierta para delimitar su utilidad e importancia en la investigación criminal. Hay que puntualizar previamente en la importancia que tiene la evidencia transformada en prueba en el proceso penal guatemalteco, esto implica a su vez una nueva herramienta para la justicia y los órganos encargados de impartirla, por lo que su incidencia en el derecho y la investigación criminal más allá de facilitar la averiguación de la verdad representa una ventana a un mundo complejo, extenso y sobre todo especializado en el cual convergen conocimientos específicos pero también la práctica y razonamiento lógico matemático son una importante variable entre lo posible y lo imposible atendiendo a la fragilidad de la evidencia digital.

López Manrique refiere que “Para la obtención de evidencia hay que estar relacionado con los diferentes medios de almacenamiento y su funcionamiento. Si se dio un delito o hay la sospecha del mismo, existen muchos medios por los cuales el delincuente pueda esconder o mover los datos y las pistas, desde un medio de almacenamiento como puede ser su computadora a un medio portátil de almacenamiento. La lista incluye memorias flash que son tan pequeñas que pueden ser llevadas en la bolsa de una prenda de vestir o la palma de la mano, también pueden ser disfrazadas como plumas, relojes digitales, cámaras digitales, chips de memoria para cámaras digitales y estos pueden ser escondidos en un sobre, PDA’s y teléfonos celulares, estos últimos pueden almacenar una variedad de información tal como mensajes de voz, mensajes de texto, notas en archivos almacenados, números

telefónicos y direcciones, así como bitácoras de llamadas perdidas, recibidas y hechas".[31] Bajo la aproximación presentada, es indispensable hare referencia a tener un conocimiento en términos adecuados de los medios de almacenamiento y cómo funcionan estos en relación a su integración física y de software para identificar las debilidades, puntualiza en la múltiple opción para ocultar o mover de ubicación datos o pistas en un dispositivo, estos pueden ir desde un computador portátil hasta una memoria flash o dispositivo usb; es larga la lista de dispositivos en los que se puede hallar evidencia digital lo que implica que conforme avanza la tecnología se modifican las técnicas para recolectar la evidencia digital; a su vez la evidencia digital adquiere diferentes formas tales como mensajes de voz, texto, notas en archivos almacenados, registro de llamadas, datos en hojas de procesamiento de texto e información personal almacenada en aplicaciones específicas ajenas al fabricante del dispositivo.

El contenido de la evidencia digital es extenso y a su vez un poco confuso ya que al integrar su concepto a la realidad se generan respuestas y preguntas más profundas sobre su forma especialmente, para Bechimol en su obra hacking desde cero refiere que "La evidencia digital, específicamente, es un tipo de prueba física, menos tangible que otras formas de evidencia (ADN, huellas digitales, componentes de computadoras, papeles). Tiene algunas ventajas sobre su contraparte no digital porque, por ejemplo, puede ser duplicada de manera exacta, es posible detectar si ha sido alterada y, aun si es borrada, a veces recuperarla. Esto se resume en: repetible, recuperable, redundante e integra".[32] Para el autor la evidencia digital es una prueba física pero menos tangible que otras evidencias y esta le da una ventaja significativa en cuanto a la identificación de alteración sustancial de su información o de su estructura, por lo que puede ser recuperada si ha sido borrada; aunque esta afirmación es circunstancial ya que los avances de la tecnología actual en informática

[31] López Manrique, Yuri Vladimir. *Computación forense: una forma de obtener evidencias para combatir y prevenir delitos informáticos*. Guatemala. Universidad San Carlos de Guatemala. 2007. Pág. 31. Disponibilidad y acceso: http://biblioteca.usac.edu.gt/tesis/08/08_0359_CS.pdf fecha de consulta: 11.08.2016.

[32] Bechimol, Daniel. *Hacking desde cero: conozca sus vulnerabilidades y proteja su información*. Buenos Aires, Argentina. RerUSERS. 2011. Pág. 39.

y sobre todo herramientas de privacidad permiten la supresión permanente de datos digitales o información al ejecutarse, sin embargo el criterio utilizado por Bechimol al describir la evidencia digital como una prueba física menos tangible atiende a su capacidad de percepción y visualización, es decir, considerar su existencia más allá de una aparente suposición y traduciéndola al plano virtual en el cual puede ser manipulable y examinada de forma adecuada.

Aunque al abordar el contenido de la evidencia digital se presentan obstáculos, el portal de informática forense de Colombia refiere que "El problema con los datos digitales es que es algo menos tangible que la mayoría de las pruebas físicas. Pertenece a la categoría de pruebas frágiles, junto con cosas tales como huellas en la nieve, porque son fácilmente destruidos o modificados. De hecho, el acto mismo de la recogida o el examen se puede cambiar. El problema con esto es que para que la evidencia sea admisible, la parte que la introducción debe demostrar que no ha sido alterado o modificado desde que fue recogida en la escena del crimen".[33] Esta problemática se deriva de la facilidad de destrucción o modificación de la evidencia digital, por lo que debe ser considerada dentro de la categoría de pruebas frágiles para el autor ya que la ausencia de tangibilidad cuestiona los criterios de perdurabilidad en determinado estado, esto infiere especialmente en la recolección o durante el análisis de la misma ya que en ese acto puede sufrir leves o significativas alteraciones la evidencia digital lo cual en su parte introductoria durante la exposición en un proceso penal, carecería de argumento válido que rectifique que esta no fue alterada o modificada desde que fue recogida en la escena del crimen.

La evidencia digital carece de tangibilidad, característica en la que diversos autores han puntualizado lo que implica que su manipulación y análisis solamente es posible a través de herramientas de informática que permitan el acceso pleno a los datos e información que se ha recolectado en la escena del crimen, aunque parte de esta afirmación implica que la escena del crimen se encuentre constituida dentro de un

[33] Informática Forense Colombia. *La evidencia digital*. Colombia. 2015. Disponibilidad y acceso: http://www.informaticaforense.com.co/index.php/la-evidencia-digital fecha de consulta: 11.08.2016.

único dispositivo y esto se entiende en lo que actualmente son los delitos informáticos, sin embargo existe un riesgo de modificación, alteración o supresión de la evidencia que en mayor o menor medida depende del investigador a cargo de la evidencia digital y de la calidad de la cadena de custodia ya que al momento de su análisis la evidencia puede sufrir cambios en su estructura o información, alcances que se deben corroborar en la parte introductoria de la exposición de la evidencia digital en los tribunales que tienen a su cargo dilucidar el delito. Ruiz Alquijay refiere que "La evidencia digital es cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático. En este sentido, la evidencia digital, es un término utilizado de manera amplia para describir cualquier registro generado por o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal".[34] En una definición más precisa Ruiz Alquijay indica que la evidencia digital para que adquiera esta denominación debe ser extraída de un medio informático, específicamente de un hardware que sea capaz de almacenar información digital por lo que necesita la intervención humana u otra semejante, aunque delimita a la evidencia digital a un sistema computacional debe entenderse que la evidencia digital por su naturaleza se puede traducir en mensajes de texto, notas de voz, llamadas de voz e información que no necesariamente se encuentra en un sistema computacional pero si se depende de uno de estos para el análisis y extracción de la información. Para su efecto la evidencia digital desde su extracción hasta su análisis debe seguir una metodología especializada que asegure que los procesos llevados a cabo puedan ser repetibles de forma sistemática, a su vez debe comprobar un carácter de idoneidad y pureza ya que por su fragilidad esta puede sufrir cambios sustanciales en su información, contenido y descripción, por ejemplo fecha de creación, fecha de modificación, autor de los datos, denominación, etc.

[34] Ruiz Alquijay, José Daniel. *La utilización de la informática forense en los casos de alto impacto social en Guatemala*. Guatemala. Universidad San Carlos de Guatemala. 2012. Pág. 57. Disponibilidad y acceso: http://biblioteca.usac.edu.gt/tesis/04/04_10450.pdf fecha de consulta: 11.08.2016.

2.3. Características de la evidencia digital

Por su naturaleza la evidencia digital a diferencia de la evidencia física presenta características muy particulares como la ausencia de tangibilidad, entre otras. Vides Álvarez cita a Brungs y Jameison en la catorce conferencia australiana de sistemas de información realizada en 2003, he indican que "La evidencia digital es única, cuando se le compara con otras formas de evidencia. A diferencia de la evidencia física, la evidencia digital es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único es su potencial de realizar copias no autorizadas de archivos, sin dejar rastro alguno. La evidencia digital posee, entre otras, las siguientes características: volátil, anónima, duplicable, alterable, modificable y eliminable".[35] La evidencia digital yace en una esfera compleja ya que por sus características su tratamiento debe ser cuidadoso y sobre todo especializado, una de las características que atraen la atención es la capacidad de ser idéntica a la original cuando se realiza una copia y sobre todo el potencial de realizar copias no autorizadas de archivos sin ser detectadas, lo que representa una compleja materia cuando se efectúan peritajes sobre información extraída de la original bajo la prevención que esta puede ser alterada o suprimida de forma sustancial.

a) Es volátil: Ya que por su estructura, programación y contenido es capaz de cambiar o variar con facilidad y de forma poco previsible; esto implica cambios en su denominación, descripción, detalles, autores y sobre todo en los datos que pudieron haber sido herramientas en la comisión de un delito.

b) Es anónima: Identificar al autor de un delito informático por ejemplo implica una compleja red de conocimientos especializados y utilización de la lógica informática ya que la evidencia digital en su forma originaria, es decir, datos o información digital puede sufrir denominaciones ilimitadas por lo que no necesariamente algunos detalles de su contenido refieren con plena certeza al

[35] Vides Álvarez, Raisa. *Evidencia digital*. Colombia. Scribd. 2011. Disponibilidad y acceso: https://es.scribd.com/doc/61944356/Evidencia-Digital fecha de consulta: 17.08.2016.

autor de dicha información; por lo que al momento de su recolección debe considerarse anónima ya que resulta en términos sencillos imposible determinar la autoría a simple inspección de una evidencia digital. Esto se puede extender a la suplantación de información o datos de forma remota, derivado de la capacidad de administrar un dispositivo de manera anónima y a una distancia considerable; por ejemplo: las instituciones tienen un departamento de mantenimiento de sistemas que tiene acceso remoto a los distintos computadores, lo cual permite la manipulación de software, datos, información y contenido media por parte de un tercero.

c) Es duplicable: Como refiere Brungs y Jameison la evidencia digital es susceptible de duplicarse de forma idéntica que el archivo original, lo que dificulta muchas veces individualizar de forma objetiva su origen; ya que aunque esta permanezca almacenada por ejemplo un documento digital sujeto a evidencia en un dispositivo usb, necesito de un dispositivo con capacidad para procesar texto lo que implica que su origen es desconocido y su autor anónimo.

d) Es alterable y modificable: Esta característica se deriva de la fragilidad de la evidencia digital ya que por su naturaleza y ausencia de tangibilidad es susceptible a ser modificable en cualquier momento, inclusive como previamente se indicó durante la cadena de custodia y análisis de la evidencia digital existe un riesgo de que la evidencia digital se altere de forma sustancial; lo que genera un complejo campo de peritaje informático en el cual los conocimientos especializados desempeñan un rol importante para la preservación, resguardo y garantía de la cadena de custodia sobre la evidencia digital.

e) Es eliminable: Una de los obstáculos que se presentan respecto a la evidencia digital es la facilidad con la que esta puede ser suprimida, hay mecanismos informáticos y herramientas que con el conocimiento necesario permiten ataques de forma remota a servidores y redes informáticas que no cuentan con la seguridad necesaria para contrarrestarlos, lo que infiere directamente en la

alteración o supresión de la evidencia digital en su momento, por lo que esta debe seguir rigurosos controles de seguridad para evitar su perdida durante la cadena de custodia ya que esto implicaría un daño directo a una tesis acusatoria por parte del ente investigador.

La evidencia digital no se limita a estas características, sino más bien suelen ser aspectos esenciales y próximos a la evidencia digital; sin embargo una de sus características complejas con el progreso de la tecnología es la capacidad de recuperar datos, información, detalles y contenido aún después de borrado, por lo que existe la posibilidad de recuperar evidencia digital de dispositivos en los cuales se pretende no dejar rastros, claro que estos alcances se logran solamente a través de la actualización constante en la informática forense y los conocimientos especializados en programación, lógica, matemática y razonamiento.

2.4. Clasificación de la evidencia digital

La evidencia digital es susceptible de clasificación, ya que en su estado original esta puede ser observada desde diferentes puntos de vista, desde documentos que contienen un simple texto, software programado para realizar funciones específicas, audio, video, hasta imágenes que al traducirlas representan o ejemplifican algo en concreto. Por lo que Harley Kozushko citado por Almeida Romo, menciona que “la evidencia digital se puede clasificar, comparar, e individualizar, es decir es el proceso por el cual se buscan características generales de archivos y datos, características que diferencian evidencia similar y que deben ser utilizadas a criterio del investigador, por ejemplo:

a) 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.
b) 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.

c) 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".[36]

Kozushko clasifica la evidencia digital atendiendo a sus características entre archivos y datos, esto implica que la clasificación de archivos sea más extensa ya que esto implica cualquier medio digital que contenga información atendiendo a las extensiones que caracterizan a los archivos (*.mp3; *.Wav; *.JPG; *.rar; *.zip; *.mp4; etc.) La clasificación que realiza Kozushko atiende a tres aspectos relevantes siendo el contenido, la función y las características propias de la evidencia digital. En la primera clasificación de la evidencia digital propone un ejemplo escueto ya que cita un e-mail y su respectiva clasificación como prioritario o con contenido spam; sin embargo desde un punto de vista amplio se puede clasificar la evidencia digital en cuanto al contenido refiriéndose a texto descriptivo o contenido numérico que se puede referir específicamente en transacciones u operaciones bancarias; por lo que la clasificación del contenido se extiende a innumerables situaciones en las cuales según la necesidad del peritaje se implementará la más adecuada.

En la segunda clasificación se refiere a que la evidencia digital puede ser clasificada en cuanto a su función, cita un ejemplo relacionado a un ataque directo proveniente de un software o virus programada para transferir información a una locación remota, lo denominan troyano y cumple funciones específicas en cuanto a su programación; puede ser destinado prácticamente a la obtención, creación, modificación o supresión de información ubicada en rutas especificas en el ordenador, por lo que su la clasificación en cuanto a su función puede ser extensa ya que el software opera según la finalidad que le ha destinado el programador. Por último, refiere que la

[36] Almeida Romo, Omar Ramiro. *Metodología para la implementación de informática forense en sistemas operativos Windows y Linux*. Ecuador. Universidad Técnica del Norte. 2011. Pág. 35, 36.

evidencia digital puede ser clasificada según sus características propias, es decir que los archivos y datos se ejecutan bajo un formato determinado por lo que se catalogan a nivel informático por su contenido y configuración, en esta clasificación es práctico señalar formatos muy reconocidos como audio, video, documentos e imágenes; sin embargo la extensión o formato de los archivos es inmensa ya que en programas o ejecutables avanzados se establecen nuevos formatos que se ejecutan según software avanzado.

Asimismo, Gómez Manrique refiere que la evidencia digital es posible dividirla en tres categorías:

a) "Registros almacenados en el equipo de tecnología informática (correos electrónicos, archivos de aplicaciones de ofimática, imágenes, etc.).
b) Registros generados por los equipos de tecnología informática (registros de auditoría, registros de transacciones, registros de eventos, etc.).
c) Registros que parcialmente ha sido generados y almacenados en los equipos de tecnología informática". [37]

Estas tres categorías son importantes ya que de forma adecuada sitúa según su naturaleza los archivos o registros informáticos almacenados en equipos de tecnología, en la primera categoría se visualizan los archivos media, correos electrónicos y documentos generados por software que procesa texto. Mientras que en la segunda categoría introduce todos aquellos archivos generados o información generada proveniente de auditorías, transacciones u operaciones bancarias y eventos las cuales son una información más sólida en cuanto a la individualización del autor de la misma y por último hace referencia a los registros generados parcialmente y que se almacenan, los mismos resultan ser complejos ya que al ser parciales implica una cadena de datos o información inconclusa y que se desconoce por lo general la fuente u origen, atendiendo a que la evidencia digital puede ser

[37] Gómez Manrique,Jonathan. *Factores que inciden en la alteración de la evidencia digital*. Colombia. 2014. Disponibilidad y acceso: http://informaticaforenseuccaraucacolombia.blogspot.com/2014/05/ensayo-factores-que-inciden-en-la.html fecha de acceso: 29.09.2016.

duplicada de forma idéntica que la original característica que atiende a las tres clasificaciones que realiza Gómez Manrique.

2.5. Importancia de la evidencia digital

La incidencia de la tecnología y los equipos informáticos ha renovado de forma drástica lo que es la investigación criminal en la actualidad. La escena del crimen y el criminal frente a las nuevas modalidades del delito se ve influido el mecanismo para la ejecución de ciertos delitos o la mayoría; desde un punto de vista socio criminal es pertinente indicar que la mayoría de delitos que son significativos para Guatemala tales como las extorsiones, secuestros, crimen organizado, asesinatos e inclusive la corrupción en todas sus formas utilizan dispositivos de tecnología para realizar una coordinación puntual para la ejecución del delito, esto implica que los rastros digitales permiten ampliar el campo de la investigación criminal y entender el delito desde un punto de partida especializado como lo es la informática forense. Por lo que la importancia de la evidencia digital radica en la oportunidad para aproximarse a la averiguación de la verdad a través de herramientas de primera tecnología, las cuales tienen como función seguir rastros según la naturaleza del delito y las circunstancias en que se cometió no limitándose únicamente a la recolección de evidencia, sino que propiamente permite iniciar investigaciones a través de movimientos sospechosos, un ejemplo de esta afirmación son las operaciones interbancarias en las cuales a pesar de existir una entidad como la Intendencia de Verificación Especial -IVE- adscrita a la Superintendencia de Bancos utiliza los rastros digitales para determinar transacciones sospechosas, al igual que en los casos de extorsión la afluencia de llamadas y la identificación en un rango determinado permiten ubicar a los individuos mediante los rastros de llamadas e intercambio constante de información entre un celular y otro, lo que le compete a la tecnología de la mano de la investigación criminal. La evidencia digital más allá de ser importante en el esclarecimiento de los hechos delictivos que por una u otra razón se ha utilizado un dispositivo de tecnología para ocultar rastros, resulta ser una necesidad en el campo de la investigación criminal ya que solo a través de esta es posible aportar medios de

convicción pertinentes que permitan generar una certeza jurídica en el juzgador al momento de emitir una resolución.

Su utilidad se ha evidenciado en los últimos años, especialmente en casos de alto impacto en Guatemala en los cuales la evidencia digital ha formado parte de la consolidación de tesis acusatorias por parte del Ministerio Público, manifestándose a través de intercambio de mensajes de texto, flujo de llamadas, individualización de transacciones financieras, operaciones con tarjetas de crédito, correos electrónicos, documentos digitales, entre otros. Por lo que su aporte al campo de la investigación criminal es significativo e implica una constante actualización en conocimientos especializados relativos a la informática forense y las metodologías adecuadas para la preservación de la evidencia digital a través de una cadena de custodia que resguarde la pureza de las evidencias recolectadas.

2.6. Diferencia entre la evidencia física y la evidencia digital

Evidencia física	Evidencia digital
Suele ser tangible	Ausencia de tangibilidad
Está compuesta por elementos susceptibles a la vista, tacto y olfato	Está compuesta de pulsos electromagnéticos y una programación que se basa en un sistema binario
Su clasificación atiende a la naturaleza del hallazgo. (Huellas, armas, etc.)	Su clasificación es extensa y atiende al formato del archivo especialmente.
Su tratamiento en Guatemala se encuentra regulada en el Manual de normas y procedimientos para el procesamiento de la escena del crimen del Ministerio Público	No cuenta con un manual en específico en el que se establezca cual debe ser el procedimiento adecuado.
Es opcional el uso de un computador para el análisis de algunas evidencias físicas.	Es indispensable el uso de un computador para efectuar su análisis.
La reproducción de la evidencia física suele ser compleja y presenta variaciones a la original	La reproducción de los archivos o evidencia digital es idéntica a la original.
Es modificable, pero fácil de identificar los cambios sustanciales.	Es frágil y fácil de modificar lo que complica determinar su pureza.
Determinar al propietario, autor o poseedor no es un proceso muy complejo.	Es anónima y su individualización es un proceso complejo.

Fuente: realizado por el investigador

Las diferencias entre la evidencia digital y la evidencia física resultan importantes para comprender los alcances de ambas, sobre todo justifica y razona la delicadeza del tratamiento de la evidencia digital a través de una cadena de custodia adecuada ya que bajo el presupuesto de la ausencia de tangibilidad resulta fácilmente modificar

la esencia de su contenido, especialmente al considerar que se necesita de un computador para realizar un análisis técnico y pertinente, lo que desencadena una compleja serie de problemas que sin duda alguna pueden afectar el contenido de la evidencia digital si el perito o especialista encargado del análisis realiza una manipulación negligente o errónea en cuanto a procedimientos. Asimismo, la evidencia digital no se encuentra exenta de ataques externos que son tan frecuentes en esta era de innovación y desarrollo de herramientas informáticas, esto implica que la evidencia digital sea susceptible de alterarse o suprimirse de forma remota si el ente investigador no cuenta con las medidas de seguridad en la red que interconecta el sistema informático de la institución.

Tal como se hace referencia en el cuadro anterior presentado, no existe un manual en específico que haga referencia cual es el procedimiento adecuado a seguir ya que en materia informática las evidencias pueden derivarse de miles de circunstancias por lo que un solo procedimiento representaría límites en el campo de la investigación criminal sobre la evidencia digital, sin embargo es indispensable puntualizar en que el encargado de analizar la evidencia digital debe reunir requisitos especiales en cuanto al manejo de la información que se le ha puesto a su disposición, ya que se presenta como barrera a la investigación criminal las multitareas que pueden realizarse por medio de herramientas de informática y dispositivos de alta tecnología por lo que el perito encargado del tratamiento de la evidencia digital debe de forma obligatoria dominar las diferentes plataformas, sistemas operativos, variedad de hardware y sobre todo software, entre otros. Por ello, es posible afirmar que la evidencia digital necesita de un tratamiento totalmente distinto a la evidencia física o tangible ya que en materia probatoria inclusive el diligenciamiento se realiza de forma diferente, especialmente porque al momento de pretender individualizar la evidencia digital resulta un proceso complejo a diferencia de otras evidencias como la sangre, huellas, cabello, entre otras.

CAPÍTULO III

RECOLECCIÓN Y ASEGURAMIENTO DE LA EVIDENCIA DIGITAL

La evidencia digital sin duda alguna es el nuevo campo de la investigación forense en la actualidad, la relación entre el ser humano, sus actividades diarias y la tecnología nunca se fue más estrecha hasta la fecha ya que tanto se ha introducido la misma en la vida de las personas que forma parte de ellas, ya sea a través de un teléfono inteligente, un computador, una tablet o cualquier dispositivo de tecnología la influencia de su utilidad se evidencia en todos y cada uno de los integrantes de las sociedades actuales. Es tan avanzada la tecnología y su influencia en lo que realizan los individuos que la misma es utilizada para cometer hechos ilícitos, esto genera nuevas técnicas de investigación criminal y para auxiliarse hace uso de la informática forense a través de procedimientos, conocimientos especializados y empíricos a fin de determinar la línea criminal.

Se genera como consecuencia de la propia investigación la denominada evidencia digital la cual se analizó en el capítulo anterior a partir de sus características, clasificación e importancia en la investigación criminal, pero para que valga la pena la evidencia digital es importante adentrarse al procedimiento de recolección y aseguramiento a través de una cadena de custodia adecuada, técnica y sobre todo profesional a fin de garantizar que los datos o información recuperada no sea modificada, suprimida o inclusive ocultada de la percepción del juzgador quien aprecia la evidencia cuando se traduce en prueba y la valora a través de la sana critica razonada, aspecto que justifica la investigación criminal en el campo de la informática forense y que resulta muy importante en el esclarecimiento de los hechos en los delitos informáticos e innumerables figuras propias del derecho penal que son influenciadas por la tecnología y en esa línea continuará hasta que la era de la tecnología empiece su declive, pierda fuerza e influencia en la vida del ser humano, mientras tanto para garantizar un proceso penal adecuado en donde la evidencia digital interactúa directamente es indispensable abordar el contenido de la

recolección y aseguramiento de esta institución. Para la recolección y aseguramiento de la evidencia digital no existe un procedimiento preestablecido en las disposiciones legales y por lo general los entes investigadores diseñan procedimientos adecuándolos a las diferentes circunstancias, por ejemplo: para la recolección y aseguramiento de la evidencia que pueda generar un teléfono móvil no se va implementar el mismo procedimiento que corresponde para una computadora y existen variables con las computadoras portátiles, ya que la diferencia de componentes, tamaños y sobre todo software hacen que varíen las circunstancias, por ello es indispensable comprender los pasos básicos para asegurar la evidencia digital a través de una cadena de custodia técnica y especializada en esta materia.

Una importante aproximación a este contenido lo realiza Cano Martínez en su obra peritaje informático y la evidencia digital en Colombia, refiere que en cuanto. En cuanto al proceso de recolección de evidencia digital, cita “en el Reino Unido se han tenido en cuenta los diversos problemas que plantea la manipulación de las pruebas electrónicas, y por ende la Asociación de Jefes de Policía (Association of Chief Police Officers - ACPO) sugiere ceñirse a un procedimiento forense estandarizado que normalmente consta de cuatro etapas:

1) Etapa de recolección: implica la búsqueda, reconocimiento, recolección y documentación de la evidencia electrónica.
2) Proceso de examen de la evidencia: como lo explica la ACPO, este proceso ayuda a hacer visible la evidencia y explica su origen y su alcance. En él se deben efectuar algunas tareas como documentar el contenido y el estado de la evidencia en su totalidad, y separar la evidencia útil de la demás información que coexista en el medio electrónico.
3) La fase de análisis: en esta etapa se inspecciona la evidencia útil obtenida del proceso de examen, indagando por su valor probatorio y relevancia.
4) El reporte o declaración: según la ACPO, el reporte debe dilucidar el proceso de examen y la información pertinente obtenida mediante dicho proceso, y contener un análisis del investigador enfocado en esos dos aspectos. En esta etapa, la asociación hace hincapié en que las notas tomadas por el examinador deben ser

preservadas para efectos testimoniales, siempre teniéndose en cuenta que el investigador podrá verse abocado a testificar también sobre la validez del procedimiento de examen de la evidencia digital y sobre sus calificaciones para conducirlo a cabalidad".[38]

El proceso de recolección y análisis de la evidencia digital tal como lo plantea Cano Martínez está diseñado según las propias necesidades que presenta la investigación criminal, se plantea como ejemplo se plantea el procedimiento estandarizado diseñado en el Reino Unido con la finalidad de superar los diversos problemas que plantea la manipulación de la evidencia digital. Como primer paso se plantea el procedimiento de la búsqueda, reconocimiento, recolección y documentación de la evidencia electrónica esto con el fin de identificar que medios se utilizaron para la materialización de un hecho delictivo y establecer la primera línea de investigación, es importante mencionar que en los casos de delitos informáticos se le puede denominar herramientas primarias ya que sin estas es imposible la comisión del delito, mientras que en otras manifestaciones del delito hay herramientas de tecnología que son auxiliares y por ello se les podría denominar secundarias ya que el resultado del delito no depende en mayor medida de la implementación de la misma y solamente generan una proximidad para la consecución del hecho delictivo.

Plantea, como segundo paso o etapa el examen de la evidencia el cual contribuye a explicar el origen y a individualizar la evidencia trazando una línea criminal respecto al alcance de la misma. Esto implica la documentación del contenido y el estado de la evidencia digital en su conjunto con la finalidad de separar la evidencia útil de la demás que coexiste en la misma unidad de almacenamiento. Seguidamente se debe concurrir a la fase de análisis y consiste básicamente en inspeccionar con las herramientas informáticas la utilidad de la evidencia digital obtenida, en este punto se indaga sobre el valor probatorio de la evidencia recabada y sobre todo la pertinencia de la misma al momento de introducirla al proceso penal. Por último en el Reino

[38] Cano Martínez, Jeimy José. *El peritaje informático y la evidencia digital en Colombia*: conceptos, retos y propuestas. Colombia. Ediciones Uniandes. 2010. Pág. 109.

Unido se requiere el reporte o declaración del perito el cual debe contener la información relativa al proceso que se implementó para analizar la evidencia digital y el resultado del análisis, haciendo énfasis en que las notas del forense en informática deben ser preservadas para efectos testimoniales. En este sentido, esta aproximación al procedimiento de recolección y aseguramiento de la evidencia digital en el Reino Unido sigue una procedimiento estandarizado con el fin de superar los problemas que presenta, circunstancia que se asocia de forma breve con otros países. Para el efecto resulta importante abordar la recolección y aseguramiento de la evidencia digital desde un procedimiento lógico y consecutivo atendiendo a la estandarización de los procedimientos de evidencias físicas o tangibles, en ausencia de un manual especializado en evidencia digital aplicable a la investigación criminal en Guatemala.

3.1. Secuestro de dispositivos de tecnología

Uno de los primeros para previo a la recolección y aseguramiento de la evidencia es el secuestro de los dispositivos considerados utilizados en la comisión de un hecho delictivo, es indispensable puntualizar en que el secuestro de los cualquier medio de tecnología que es objeto de la informática forense debe seguir procedimientos legales preestablecidos, en este sentido en aras de proteger los derechos de las personas y proteger especialmente la intimidad, propiedad privada y darle cumplimiento a un debido proceso, es posible efectuar el secuestro de bienes solamente a través de orden judicial con el fin de proteger de arbitrariedades a la población y garantizar el cumplimiento de los derechos reconocidos constitucionalmente. Es por ello, que el secuestro de los dispositivos de tecnología es una de las diligencias más importantes en el manejo de la evidencia digital ya que sin el acceso autorizado por un juez competente toda la información o datos obtenidos resultan inútiles al pretenderse integrar a un proceso penal debidamente instruido, en el cual la evidencia digital según la naturaleza del delito juega un papel fundamental para condenar o absolver al acusado. Gómez Manrique refiere que “La evidencia digital es el objetivo más importante en la aplicación de la informática forense, consiste en la búsqueda y recopilación de información, aparejado con el

proceso de identificación del incidente. El personal encargado debe actuar de forma metódica y profesional antes de realizar la búsqueda de señales o evidencias del delito para que esta no conlleve a una eliminación de huellas. Excluyendo la posibilidad de realizar un análisis forense de lo sucedido que le permita contestar a las preguntas de ¿qué?, ¿cómo?, ¿quién?, ¿de dónde? y ¿cuándo?, impidiendo incluso llevar a cabo acciones legales posteriores".[39] La justificación del secuestro de los dispositivos de tecnología para el tratamiento de la evidencia digital se fundamenta en que como parte de la informática forense necesita métodos profesionales para la búsqueda de las evidencias relacionadas al delito, por ello es que al realizar un análisis forense sobre la evidencia digital de forma profesional es posible contestar las presuntas señaladas y a su vez permite llevar las acciones legales correspondientes dentro del proceso penal. Esta actividad tiene su fundamento en el artículo 198 del Código Procesal Penal guatemalteco decreto 51-92 de la Congreso de la República el cual bajo el nombre de Entrega de cosas y secuestro dispone "Las cosas y documentos relacionados con el delito o que pudieran ser de importancia para la investigación y los sujetos a comiso serán depositados y conservados del mejor modo posible. Quien los tuviera en su poder estará obligado a presentarlos y entrega los a la autoridad requirente. Si no son entregados voluntariamente, se dispondrá su secuestro". Es importante concebir la idea de que las computadoras, teléfonos inteligentes, tablets y cualquier otro dispositivo de tecnología que sea posible utilizar en un delito que contenga información valiosa para la búsqueda de la verdad, debe ser secuestrado en circunstancias muchas veces inmediatas a fin de evitar que se pueda eliminar o suprimir los rastros del delito.

Para realizar el secuestro de cualquier dispositivo de tecnología que se considere que contenga información o datos que puedan ser útiles para la investigación es indispensable observar lo preceptuado en artículo 200 del Código Procesal Penal bajo el nombre de Orden de secuestro el cual indica que "La orden de secuestro será expedida por el juez ante quien penda el procedimiento o por el presidente, si se

[39] Gómez Manrique, Jonathan. *Óp. cit.* pág. 8.

tratare de un tribunal colegiado. En caso de peligro por la demora, también podrá ordenar el secuestro el Ministerio Público, pero deberá solicitar la autorización judicial inmediatamente, consignando las cosas o documentos ante el tribunal competente. Las cosas o documentos serán devueltos, si el tribunal no autoriza su secuestro", en la labor de investigación criminal es importante observar los preceptos legales y formalidades que exigen las normas procedimentales, por lo que no seguir los requisitos que se encuentran establecidos en la ley la evidencia digital al momento de integrar al proceso penal para su valoración en su manifestación de prueba digital sería rechazada por ilicitud o ilegalidad, por lo que el secuestro de los dispositivos de tecnología en los que se presume que existen indicios o evidencias de la comisión de un delito que es perseguido por la ley, se debe considerar que para acceder a un dispositivo y secuestrarlo se debe realizar con orden de juez competente quien decide si con lo información circunstancial que le presenta por parte del ente investigador es pertinente efectuar el secuestro ya que de por medio esta un derecho garantizado por la Constitución Política como lo es la privacidad e intimidad anexado a la inviolabilidad de la vivienda. Como parte de un estudio objetivo y en ausencia de un manual o guía por parte del Ministerio de Público de Guatemala para el manejo de la evidencia digital en la investigación criminal resulta importante utilizar como auxiliar la guía No. 13 sobre seguridad y privacidad de la información que se centra en la evidencia digital del Ministerio de Tecnologías de la Información y Comunicaciones de Colombia, el cual contiene importantes lineamientos vinculantes en la investigación criminal en el país sudamericano y el manejo de la evidencia digital a través de la estandarización de un procedimiento adecuado.

3.2. Creación del archivo / bitácora de hallazgos (cadena de custodia)

Previo a iniciar cualquier diligencia relacionada a la evidencia digital, posterior al secuestro de los dispositivos de tecnología que se consideren sospechosos en la realización de un hecho delictivo, es indispensable que el informático forense maneje una bitácora de hallazgos, la cual para el Ministerio de Tecnologías de la Información y Comunicaciones de Colombia inicia la cadena de custodia en lo que se refiere a la evidencia digital. Esta consiste "en la creación y aseguramiento de un documento, ya

sea físico o electrónico, que permita llevar un historial de todas las actividades que se llevan a cabo durante el proceso, y de los hallazgos encontrados, de modo que se tenga un resumen que permita hacer la reconstrucción del caso tiempo después de que este haya sido analizado".[40] La bitácora de hallazgos aplica en la investigación criminal tradicional y en la informática en lo que se refiere archivos electrónicos, por lo que resulta importante llevar un historial de las actividades así como de los indicios o evidencias que se van a someter a investigación, esto facilita refiere el Ministerio de Tecnologías de la Información y Comunicaciones de Colombia la reconstrucción del caso cuando se haya analizado la información de forma pertinente, adecuada y de forma técnica ya que la creación de la línea del tiempo en cuanto a la forma en que se utilizó un dispositivo de tecnología en la comisión de un delito resulta importante para explicar y justificar la evidencia digital. Es importante llevar un historial de hallazgos por medio de una bitácora ya que esta es posible que deba presentarse al momento de diligenciar la prueba digital dentro del proceso penal, a fin de que el juez pueda determinar los alcances de la misma para su apreciación y posterior valoración a través de la sana critica razonada.

3.3. Proceso de identificación y detección de la evidencia digital

Este paso es uno de los más importantes ya que implica la identificación y detección de la evidencia digital, ya que de acuerdo a los mismos sistemas operativos existen miles de archivos que son propios y funcionales para el arranque de cada sistema operativo, por lo que existe una serie de archivos que no son útiles como evidencia digital. Asimismo, es indispensable la manipulación de los diversos sistemas operativos por lo que es necesario identificarlo de forma adecuada ya que los conocimientos entre una plataforma operativa y otra varía significativamente, esto implica a su vez la identificación de particiones de almacenamiento de información y datos informáticos lo que representa un extenso proceso de identificación de información y detección de datos relacionados al delito objeto de investigación.

[40] Ministerio de Tecnologías de la Información y Comunicaciones de Colombia. *Guía No. 13: sobre seguridad y privacidad de la información que se centra en la evidencia digital*. Colombia. MINTIC. 2016. Pág. 19.

3.3.1. Determinación del sistema operativo y las aplicaciones instaladas

Identificar el sistema operativo en el cual se realizará es indispensable, ya sea en dispositivos móviles o computadores la diversidad de OS atienden a la manufactura de las distintas compañías fabricantes de plataformas para la manipulación de los dispositivos de tecnología, por lo que el informático forense debe tener conocimientos avanzados en los diversos sistemas operativos así como en las aplicaciones instaladas en un dispositivo o computador ya que la complejidad del manejo de aplicaciones e inclusive de los diversos sistemas se le presentan a los profesionales ingenieros en sistemas, por ejemplo: en cuanto a sistemas operativos de computadores existe una diversidad como lo es Linux, Ubuntu, Windows, MAC, Unix, Fedora, Solaris, etc. Los cuales no se rigen bajo las mismas reglas de programación y utilidad por lo que es importante la preparación en este campo del informático forense a fin de garantizar una adecuada cadena de custodia. Se considera que "al determinar el sistema operativo y las aplicaciones instaladas, se está en la capacidad de obtener la lista de compendios criptográficos de los archivos típicos del sistema operativo y de las aplicaciones, para verificar posteriormente la integridad de los estos archivos de encontrarse en la imagen sometida a análisis. El objetivo de este paso es descartar información que no será relevante para analizar. Con la lista de compendios criptográficos obtenida, se procede a verificar la integridad de los archivos en la imagen que aparecen en tal lista. Si dicha comprobación es exitosa, estos archivos se consideran "buenos" y por lo tanto son descartados del proceso de análisis en la fase posterior",[41] al determinar el sistema operativo el técnico en informática forense puede o no llevar a cabo una recolección de la evidencia digital, es importante puntualizar que a pesar que hay sistemas operativos que son más utilizados que otros este debe poseer conocimientos avanzados en la mayoría de plataformas operativas en dispositivos de tecnología ya que de esto depende una diligente recolección de la evidencia digital y de los indicios que se desprendan de la investigación criminal.

[41] *Ibíd.* Pág. 22.

3.3.2. Identificación de las particiones actuales y anteriores

Seguidamente es importante identificar la cantidad de particiones, es decir las unidades de almacenamiento con las que cuenta un dispositivo de tecnología, “La identificación de las particiones en un dispositivo es de vital importancia, ya que reconocerlas implica la identificación de su sistema de archivos, mediante el cual se pueden reconocer características especiales de la organización de la información y se puede definir la estrategia de recuperación de archivos adecuada. Se debe proceder a hacer un análisis para determinar si representan algún tipo de información relevante para la investigación. En caso de estar protegidos, estos archivos serán tenidos en cuenta en la fase de la identificación de archivos protegidos, de lo contrario, se incluirán en el conjunto de archivos potencialmente analizables”.[42] Es fundamental que se realice una identificación de las particiones de un dispositivo, ya que es posible establecer almacenamientos propios de los dispositivos y externos los cuales podrían contener información relevante para la investigación criminal, asimismo es en este punto donde se define la estrategia de recuperación de archivos, información y datos de diversa naturaleza que son considerados potencialmente analizables y es posible separar la información protegida de la libre la cual necesita otro tipo de estrategia y herramientas para acceder a la información que contiene. Esto implica que para cada una de las particiones identificadas, se debe establecer el sistema de archivos que cada una cuenta ya sea FAT, NTFS y HPFS los más comunes.

3.3.3. Recuperación de los archivos borrados

Una de las características de la evidencia digital es que es fácil de modificar o eliminar, lo que implica que representa un serio obstáculo en la investigación criminal; los mismos avances tecnológicos y los distintos desarrolladores de software convencional han diseñado programas para la recuperación de archivos que aparentemente se han suprimido en su totalidad de los discos de almacenamiento, sin embargo hay sectores en las particiones que almacena información recuperable que aparentemente se ha borrado de forma voluntario o errónea, durante esta

[42] *Ibíd.* Pág. 20.

actividad “se deben tratar de recuperar los archivos borrados del sistema de archivos, lo que es conveniente dado el frecuente borrado de archivos para destruir evidencia. Dependiendo de las características técnicas y del estado del sistema de archivos puede no ser posible la recuperación de la totalidad de los archivos eliminados, por ejemplo si estos han sido sobre escritos, o si se han utilizado herramientas de borrado seguro para eliminarlos. Los archivos recuperados exitosamente formarán parte de los archivos potencialmente analizables, exceptuando los archivos identificados como protegidos que serán tenidos en cuenta durante la fase de identificación de archivos protegidos”.[43] Uno de los más complejos problemas a los que se enfrenta la investigación criminal en cuanto a la evidencia digital es la supresión de archivos y borrado de información como mecanismo para la destrucción de los indicios relacionado a la comisión de un delito, sin embargo el técnico en informática forense debe tener conocimientos avanzados sobre la recuperación de archivos eliminados como parte de una adecuada investigación criminal, esto implica que aunque no es posible recuperar la totalidad de archivos eliminados especialmente aquellos que han sido suprimidos por medio de herramientas de borrado seguro es un procedimiento que no se puede obviar con la finalidad de identificar información eliminada, recuperable y potencialmente analizable.

Por su parte Gómez Manrique refiere que “una vez realizada una exploración de los ficheros existentes, se deberá utilizar un programa de recuperación de ficheros borrados (como el programa Revive) para localizar potenciales ficheros relevantes que hubiesen sido borrados. El los discos ópticos, se puede grabar a continuación de lo ya grabado, haciendo inaccesible lo anterior: también se deberán revisar estas grabaciones previas, si existiesen”.[44] Plantea como ejemplo del proceso de exploración e identificación de información potencialmente analizable y la implementación de programas o herramientas de recuperación de información relevante que hubiese sido borrada por el sindicado e inclusive un tercer, por lo que

[43] *Ibíd.* pág. 21.
[44] Gómez Manrique, Jonathan. *Óp. cit.* pág. 10.

se presentan problemas adicionales como lo es en los discos ópticos regrabables en los cuales la información puede ser sobrescrita haciendo la información anterior inaccesible al investigador forense que busca indicios o evidencias digitales según la naturaleza del delito.

3.3.4. Consolidación de archivos potencialmente analizables

Dentro del proceso de identificación y detección de evidencia digital es importante consolidar la información, datos, archivos de diversas extensiones y cualquier otra secuencia informática que pueda resultar potencialmente analizable para establecer la línea de tiempo criminal, el Ministerio de Tecnologías de la Información y Comunicaciones de Colombia refiere que "durante esta fase se reúnen todos los archivos encontrados durante las fases de recuperación de archivos borrados, recuperación de información escondida, identificación de archivos no borrados e identificación de archivos protegidos".[45] Esta fase consiste en la reunión de toda la información, datos o archivos obtenidos e identificados potencialmente analizables en relación con un hecho delictivo en el cual se hayan utilizado dispositivos de tecnología, es en esta fase donde es posible clasificar y dividir los archivos considerados evidencia digital en las diferentes categorías que se presenta a continuación:

a) "Archivos "Buenos" Modificados: Son identificados en la fase de filtrado como archivos buenos cuya versión original ha sido modificada.

b) Archivos "Malos": Se obtienen a partir de la comparación de los archivos sospechosos contra los compendios criptográficos de archivos "malos" relacionados con el sistema operativo particular. Estos archivos representan algún tipo de riesgo para el sistema en el que se encuentran o se ejecutan, por ejemplo: sniffers, troyanos, backdoors, virus, keyloggers entre otros.

[45] Ministerio de Tecnologías de la Información y Comunicaciones de Colombia. *Óp. cit*. pág. 22.

c) Archivos Con Extensión Modificada: Aquellos cuya extensión no es consistente con su contenido (para ello siempre es necesario verificar los encabezados de los archivos y no su extensión)".[46]

Estas tres clasificaciones son el resultado la búsqueda de información borrada, modificada y con un grado de seguridad que dificulta su acceso que se ha considerado potencialmente analizables, pero especialmente con un vínculo en la comisión del delito objeto de investigación criminal ya que son archivos prioritarios para el análisis porque son considerados sospechosos de haber sido modificados para no ser detectados o simplemente para ocultar cualquier rastro que vincule con la comisión de un delito.

El proceso de identificación y detección de la evidencia digital es uno de los más complejos, ya que convergen extensos conocimientos en sistemas operativos, sistemas de archivos, particiones y todo lo referente a la individualización de archivos, documentos, datos, extensiones e información que es objeto de investigación criminal; por su parte el informático forense debe ser un profesional con conocimientos especializados en cada área, en especial a la que se refiere a la recuperación de información modificada o eliminada ya que de esto depende identificar los vestigios de un delito cometido con el auxilio de un dispositivo de tecnología.

3.4. Recolección de los indicios y evidencia digital

La recolección de los indicios y evidencia digital es una de las etapas más delicadas en la investigación criminal en lo que se refiere a los dispositivos de tecnología, es indispensable tomar en cuenta la facilidad de alterar los datos e información digital por lo que siempre es recomendable hacer un respaldo completo de dicha información con la finalidad de no afectar la original, tomando en cuenta la característica que la evidencia digital es duplicable e idéntica a la original, por lo que se han diseñado distintos dispositivos que contribuyen a la recuperación y

[46] *Ibíd.* pág. 23.

recolección de la evidencia digital, básicamente es posible indicar que para la recolección de la evidencia digital es necesario contar con una unidad de almacenamiento externa que permita duplicar la información y datos de forma idéntica a la original para posteriormente someter a un análisis forense, sin embargo los dispositivos tradicionales son inseguros y solamente sirven como unidad de alojamiento de información o un respaldo con un nivel de seguridad mínimo ya que se realiza una extracción directa, lo que no garantiza una cadena de custodia adecuada, es por ello que en el mercado se han desarrollado herramientas de informática y hardware que cuentan con un sistema de recolección y extracción de información de los discos de almacenamiento o memoria de almacenamiento de los dispositivos, entre las herramientas utilizadas en el análisis forense de dispositivos de tecnología según el perito judicial informático Sánchez Cordero se pueden mencionar los siguientes:

a) “UFED Standard.
b) XRY.
c) Mobilyze.
d) SecureView2.
e) MobilEdit!
f) Oxygen Forensic.
g) CellDEK.
h) Mobile Phone Examiner.
i) Lantern.
j) Device Seizure.
k) Neutrino”.[47]

Esta serie de herramientas son en su generalidad utilizadas para la extracción y recolección de información de dispositivos móviles que se consideran que han sido

[47] Sánchez Cordero, Pedro. *Forensics powertools (listado de herramientas forenses).* 2013. Disponibilidad y acceso: http://conexioninversa.blogspot.com/2013/09/forensics-powertools-listado-de.html fecha de consulta: 02.10.2016.

utilizados en la comisión de un hecho delictivo, sin embargo en lo que se refiere a computadoras o portátiles se presenta un complejo procedimiento ya que la variedad de sistemas operativos y las rutas de seguridad pueden ser modificadas por el usuario o administrador de los dispositivos, mientras que en materia de móviles las plataformas de sistemas operativos más comerciales son Windows mobile, IOS, Android y blackberry por lo que diseñar los dispositivos o herramientas para la recolección de la información identificada como sospechosa o catalogada como evidencia digital ha sido un reto de complejidad regular, esto permite estandarizar los procedimientos para la recolección a través de la implementación de ciertas herramientas como lo es el UFED, sin embargo en la esfera de la computación las empresas manufactureras de los sistemas operativos han creado rutas de seguridad que solo pueden ser saltadas por alguien con conocimientos especializados, en especial en sistemas que no son comunes o comerciales que manejan código abierto lo cual le permiten al usuario o administrador del dispositivo modificar la seguridad y rutas de información, así como extensión de los archivos con la finalidad de ocultar información importante.

Por su parte, Leonardo González hace mención en su artículo veintiún herramientas populares de informática forense a marco digital forensics, la cual “es una popular plataforma dedicada al análisis forense digital. La herramienta es de código abierto y está bajo licencia GPL. Se puede utilizar ya sea por profesionales o no expertos sin ningún problema. Puede ser utilizado para la cadena de custodia digital, para acceder a los dispositivos remotos o locales, los forenses de Windows o el sistema operativo Linux, la recuperación de archivos borrados, escondidos, búsqueda rápida de los metadatos de archivos, y varias otras cosas. EnCase es otra de usos múltiples plataforma forense popular entre muchas herramientas buenas para varias áreas del proceso forense digital. Esta herramienta puede recopilar rápidamente datos de varios dispositivos y desenterrar la evidencia potencial. También produce un informe basado en la evidencia. Esta herramienta no viene de forma gratuita. La licencia

cuesta 995 dólares".[48] Estas dos herramientas son un ejemplo de las múltiples opciones que ofrece el mercado de la investigación criminal en su manifestación de la informática forense, lo que implica que su utilidad resulta importante pero su implementación se limita a ciertas plataformas, en el caso de marco digital forensics solamente puede ser utilizada en sistemas operativos Windows y Linux, excluyendo de su uso otros sistemas como Ubuntu, Unix, Mac, entre otros

3.4.1. Dispositivo UFED

Para tener una aproximación de cómo funciona la recolección de indicios y evidencia digital en la investigación criminal, se abordará de forma didáctica el dispositivo UFED que es el que se implementa en Guatemala para extraer la información relevante de los dispositivos móviles y de forma inmediata crea una cadena de custodia que garantiza la pureza de la información obtenida de un teléfono celular inteligente. El dispositivo UFED "Es un conjunto de aplicaciones práctico, flexible y rentable para cualquier personal de investigaciones o de inteligencia que necesite un kit de herramientas forense de dispositivos móviles en su PC o laptop. Basada en tecnología de software UFED comprobada, UFED 4PC le proporciona a los usuarios capacidades de avanzada para realizar extracción de datos, decodificaciones y análisis de una amplia gama de dispositivos móviles sobre una plataforma única".[49] Tal como refiere el fabricante de este dispositivo, es un conjunto de aplicaciones que se orienta a la extracción de información de dispositivos móviles y permite el análisis de diversos sistemas operativos que se encuentran en el mercado de la comunicación móvil, entre sus principales características se pueden señalar la "Solución integral de análisis forense de dispositivos móviles, flexible y práctica para la investigación Incomparable soporte de dispositivos Android, iOS y BlackBerry®; basada en tecnología UFED comprobada, le brinda a los usuarios todas las capacidades de extracción física, lógica y del sistema de archivos; cargadores de

[48] González, Leonardo Emmanuel. *21 herramientas populares de informática forense*. 2014. Disponibilidad y acceso: https://prezi.com/kcoki3kq5wsj/21-herramientas-mas-populares-de-informatica-forense/ fecha de consulta: 02.10.2016.

[49] Cellebrite delivering mobile expertise. *UFED 4PC*. Estados Unidos. 2013. Pág. 2. Disponibilidad y acceso: http://www.complexbiz.com/wp-content/uploads/2014/05/UFED-4PC-Brochure_AL_ES_web.pdf fecha de consulta: 02.10.2016.

arranque personalizados para asegurar extracciones adecuadas desde el punto de vista forense; su exclusivo motor de verificación de evidencias permite la validación de datos recuperados".[50] Estas importantes características definen la utilidad en la investigación forense del dispositivo UFED en Guatemala, para lo cual se debe seguir un procedimiento interinstitucional para su implementación y solicitud ya que no en todas las fiscalías del país se cuenta con este dispositivo por su alto costo, sin embargo es una herramienta eficaz para la extracción física, lógica y del sistema de archivos que auxilia en la informática forense la línea de tiempo criminal, con la finalidad de averiguar la verdad y ser posible integra la prueba digital dentro del proceso penal guatemalteco.

3.5. Transporte y entrega de la evidencia digital

Para el transporte y la entrega de la evidencia digital se deben seguir los pasos establecidos en la investigación criminal tradicional, se debe observar la instrucción 104, 105, 106, 107 del Manual de normas y procedimientos para el procesamiento de la escena del crimen del Ministerio Público de Guatemala el cual indica respecto al traslado de las evidencias lo siguiente: "el técnico embalador remite los indicios al laboratorio, a través del formato de la DICRI número URE-02-Solicitud de análisis, entrega de indicios, cadena de custodia en el que consignará los datos del caso, indicando el tipo de análisis solicitado, conforme instrucciones del fiscal a cargo… El técnico embalador entrega los indicios al lugar a donde corresponda, de no requerir ningún análisis, los indicios deberán remitirse a través del formulario URE-02.

1. En la ciudad Capital, se entregan directamente al Almacén Central de Evidencias.

2. en los demás municipios y departamento, se entregan a la bodega de evidencias de la fiscalía municipal o distrital, para su posterior traslado, en condiciones de seguridad, al Almacén Central de Evidencias en la Ciudad Capital".

[50] *Loc. cit.*

Los formatos tienen incluido el registro de cadena de custodia y deben ser firmados y sellados por el embalador y el Fiscal a cargo. El Fiscal como responsable legal de la custodia de los indicios, una vez embalados es quien ordena hacia donde se remiten:

a. “Dinero, valores: a la bóveda de valores del Ministerio Público; de conformidad con el monto incautado, coordinará su traslado con el Encargado del Almacén Central de Evidencias y el Jefe del Departamento de Seguridad del Ministerio Público, en los términos que establece el normativo para la guarda, custodia y conservación de evidencias en la bóveda del Ministerio Público, aprobado por acuerdo 37-2008 y la instrucción 011-2008 de fecha 28 de agosto de 2008, emitida por el jefe administrativo.
b. Drogas, fármacos o estupefacientes, precursores o similares: a la Subdirección General de Análisis e Información Antinarcótica -SDGAIA- a través de la Policía Nacional Civil.
c. Vehículos: a la bodega de inspección vehicular del Ministerio Público o en su defecto, a los predios de la PNC.
d. Armas de fuego: Deberán ser remitidas al INACIF
e. Los indicios que requiera otro tipo de análisis especial se remiten a donde corresponda según su naturaleza”.

Por la naturaleza de la evidencia digital se debe remitir al Instituto Nacional de Ciencias Forenses de Guatemala, institución que tiene a su cargo el análisis forense de los datos, archivos e información obtenida de dispositivos de tecnología, se observa que dentro del Manual de Normas y Procedimientos para el Procesamiento de la Escena del Crimen del Ministerio Público no existe una instrucción específica sobre el transporte y entrega de la evidencia digital, por lo que en su defecto debe ser remitida con las mismas formalidades y requisitos a la institución encargada de la investigación forense en Guatemala.

3.6. Análisis de la evidencia digital

Al superar las fases anteriores ya con la evidencia digital en la institución encargada de su guarda y custodia es posible realizar el análisis respectivo valiéndose de las

herramientas de informática, así como de los controles de seguridad para garantizar que los datos, archivos y la información considerada sospechosa no puede ser alterada o borrada para entorpecer la investigación criminal, para su efecto el Ministerio de Tecnologías de la Información y Comunicaciones de Colombia refiere que en "esta fase se realizará un análisis de la información que logró extraerse de las diferentes fuentes y que se considera relevante o prioritaria para ser estudiada (después de realizar la depuración en las fases anteriores). Dicho análisis puede involucrar y relacionar los eventos, archivos, logs, testimonios, fotografías, videos de vigilancia etc… para así llegar a alguna conclusión determinada".[51] El análisis de la evidencia digital puede versas sobre diferentes puntos con el fin de alcanzar una conclusión centrada en la línea de tiempo del delito, ya que según las condiciones del hecho criminal no siempre el análisis versa sobre los puntos racionales y lógicos de la información sustraída, tal es el caso de los delitos informáticos en contraste con delitos tradicionales que utilizan la tecnología para facilitar la comisión de un hecho delictivo. Es por ello, que el análisis de la evidencia digital permite crear patrones identificables relacionados al delito objeto de investigación criminal, es una de las etapas más importantes ya que en esta fase se define la utilidad de la evidencia digital dentro del proceso penal en su etapa probatoria en el debate y se puede concluir respecto a su valoración, pertinencia y relación causal con el delito imputado por el ente investigador.

El analista forense especializado en informática y computación debe valerse de las herramientas pertinentes para realizar las conclusiones adecuadas respecto a lo que se investiga, sin embargo este debe dominar en una amplia esfera los procedimientos válidos para el análisis de la evidencia digital ya que el mismo puede ser llamado a modificar, ampliar o ratificar las conclusiones del análisis de la evidencia digital, pudiendo ser sometido a contradictorio según las reglas del proceso guatemalteco.

[51] Ministerio de Tecnologías de la Información y Comunicaciones de Colombia. *Óp. cit.* Pág. 26.

3.7. Fase de reporte de evidencia digital

En observancia de la guía No. 13 sobre seguridad y privacidad de la información que se centra en la evidencia digital del Ministerio de Tecnologías de la Información y Comunicaciones de Colombia coloca como última fase de la recolección y aseguramiento de la evidencia digital, la fase de reporte que debe brindar el perito en informática forense como resultado de las diligencias o fases anteriores procurando conservar la pureza de los datos, archivos e información relacionada a la investigación criminal, este último paso justifica las actuaciones relacionadas a la evidencia digital y sobre todo pone de manifiesto la pertinencia de la evidencia digital transformada en prueba digital que debe presentarse e integrarse de forma adecuada y legal al proceso penal guatemalteco en su etapa del debate para que sea apreciada por el juzgador y posteriormente valorada a través de la sana critica razonada, se considera que es "la fase final del procedimiento de evidencia digital es el reporte, el cuál presenta toda la información y la evidencia obtenida en la fase de análisis. Este reporte debería contemplar los siguientes aspectos:

- Resultado de los análisis.
- Cómo y por qué fueron utilizadas las diferentes herramientas y procedimientos para recolectar y analizar la información, eso sustentará el trabajo realizado.
- Se debe tener en cuenta la audiencia a la cual se presentará el informe, dado que si debe presentarse a nivel gerencial, el contenido técnico no debe tener la misma densidad que para un grupo de ingeniería, ya que en este punto es probable que se deba indicar exactamente ¿Qué ocurrió?, ¿En qué plataforma?, ¿Qué fue realizado?, sus consecuencias y las posibles contramedidas para evitar que ocurra nuevamente.
- Acciones a tomar (si es para remediar algún incidente o crimen), como por ejemplo mejorar determinados controles de seguridad, reducir alguna vulnerabilidad encontrada, refuerzo en el entrenamiento del personal (sea usuario final o equipo de respuesta a incidentes), todo esto depende de contexto del incidente.

- Determinar si es necesario realizar más estudios para llegar a una conclusión definitiva o si únicamente es posible llegar a explicaciones alternativas o hipótesis, estas deben ir plasmadas en el documento con su justificación respectiva.
- Recomendaciones relacionadas a mejoramiento en las políticas, procedimientos, herramientas de detección y otras observaciones para mejorar el proceso forense".[52]

Aunque en Guatemala el contenido de la evidencia digital aún es complejo y la inexistencia de un manual o guía en específico que indique la presentación del reporte y análisis de los datos, información y archivos objeto de investigación criminal es importante tomar en cuenta de forma auxiliar lo anterior, ya que el técnico en informática forense debe justificar las herramientas implementadas en el análisis de los indicios y la evidencia digital con la finalidad de crear la certeza jurídica relacionada a la pureza de las afirmaciones concluyentes, sobre todo lo que se relaciona a la identificación, recolección y la individualización de dicha evidencia así como el vínculo con el delito objeto de investigación criminal, la forma del reporte que presenta la guía de Colombia puede sufrir variaciones ya que los ciclos, periodos, métodos, herramientas, procedimientos y mecanismos implementados para la investigación en Guatemala pueden ser similares pero no idénticos, pero en ausencia de una guía estandarizada desarrollada con la finalidad de vencer los obstáculos que versan sobre la evidencia digital debe observarse de forma auxiliar.

Es sin duda alguna, un procedimiento complejo que desde el secuestro de los dispositivos de seguridad se debe garantizar la cadena de custodia a través de la bitácora de hallazgos hasta el momento en que se introduce la evidencia digital como prueba en el proceso penal guatemalteco, esto como finalidad suprema de la investigación criminal y su objetivo de la averiguación de la verdad a través de los medios de prueba legales, pertinentes y lícitos en todas sus manifestaciones.

[52] *Ibíd.* Pág. 28.

3.8. La cadena de custodia de la evidencia digital

La evidencia digital es un importante paso en la evolución de la investigación criminal en la actualidad, esto implica procedimientos complejos y especialmente un conjunto de conocimientos profesionales y especializados para asegurar la pureza de la evidencia sometida a investigación, es por ello que la cadena de custodia desempeña un papel importante en la informática forense ya que solo a través de esta es posible justificar la licitud de la evidencia, mientras que los riesgos de alteración o supresión de esta pueden disminuirse, Bechimol en su obra hacking desde cero refiere que "durante todo el proceso será fundamental conservar lo que se denomina cadena de custodia, es decir, todas las manos por las que pasa la evidencia y que procesos sigue mientras se trabaja con ella. Un atacante que pueda alterar la cadena de custodia podría obtener acceso a la implantación de falsas pruebas y modificar la evidencia. El atacante y el investigador estarán enfrentados en lo referido a la informática forense, y el que posea mayores conocimientos sobre determinados temas, tendrá mejores posibilidades de cumplir con su objetivo".[53] El autor hace referencia a que la cadena de custodia debe conservarse durante todas las intervenciones o diligencias que se realicen sobre la evidencia digital esto implica llevar un estricto control respecto a quien manipula los datos, archivos e información sujeta a investigación criminal, ya que es posible que un atacante pueda alterar la cadena de custodia y alterar la información o implantar falsos datos lo que modificaría el rumbo de la investigación conjuntamente con la imputación y el resultado del proceso penal.

Para el Ministerio de Tecnologías de la Información y Comunicaciones de Colombia la cadena de custodia de la evidencia digital "es un procedimiento que debe tenerse en cuenta desde el mismo instante que se decida realizar el proceso de evidencia forense, ya que este procedimiento, basado en el principio de la "mismidad", tiene como fin garantizar la autenticidad e integridad de las evidencias encontradas en alguna situación determinada, es decir, que lo mismo que se encontró en la escena,

[53] Bechimol, Daniel. *Óp. cit.* Pág. 43, 44.

es lo mismo que se está presentando al tribunal penal. La información mínima que se maneja en una cadena de custodia, para cualquier caso, es la siguiente:

- Una hoja de ruta, en donde se anotan los datos principales sobre descripción de la evidencia, fechas, horas, custodios, identificaciones, cargos y firmas de quien recibe y quien entrega;
- Recibos personales que guarda cada custodio y donde están datos similares a los de la hoja de ruta.
- Rótulos o etiquetas que van pegados a los empaques de las evidencias, por ejemplo a las bolsas plásticas, sobres de papel, sobres de Manila, frascos, cajas de cartón, etc.
- Libros de registro de entradas y salidas, o cualquier otro sistema informático que se deben llevar en los laboratorios de análisis y en los despachos de los fiscales e investigadores.
- Esta trazabilidad, brindará la confianza suficiente a quienes reciban las evidencias para certificar que toda la información ha conservado su integridad, que no ha sido alterada o modificada".[54]

La cadena de custodia debe tenerse en cuenta desde la primera diligencia relacionada a la evidencia digital, en observancia de un principio denominado mismidad que consiste en que "es necesario tener la completa seguridad de que lo que se traslada, lo que se mide, lo que se pesa y lo que se analiza es lo mismo en todo momento, desde el instante mismo en que se recoge del lugar del delito hasta el momento final en que se estudia y destruye… el gran problema que plantea la cadena de custodia es justamente garantizar que desde que se recogen las evidencias (en nuestro caso, digitales), relacionadas con el delito, hasta que éstas llegan a concretarse como prueba en el momento del litigio, el elemento sobre el que recaerán los principios de inmediación, publicidad y contradicción, tanto de las partes como de los juzgadores, es el mismo".[55] Es por ello que la cadena de custodia es de

[54] Ministerio de Tecnologías de la Información y Comunicaciones de Colombia. *Óp. cit.* Pág. 15.
[55] García, José Aurelio. *Cadena de custodia vs mismidad*. España. Informática Profesional Salmantina. 2016. Disponibilidad y acceso: http://www.informaticoforense.eu/cadena-de-custodia-vs-mismidad/ fecha de consulta. 02.10.2016.

gran importancia para el manejo de la evidencia digital, ya que se debe garantizar que las evidencias recogidas son las mismas que se han sometido a un análisis criminal y que no ha sufrido variaciones significativas en su contenido o en los datos que han sido objeto de investigación por parte del perito en informática forense. De ello, el principio de mismidad garantiza a las partes procesales e inclusive al juzgador o tribunal que la evidencia transformada en prueba digital es la misma que se ha recogido en la escena del crimen, la que se ha estudiado, analizado, derivado conclusiones y hasta el momento en que se introduce al proceso penal de forma legal ya que como parte de su naturaleza probatoria, interactúan los principios de inmediación, publicidad y contracción aspectos que son determinantes para garantizar un debido proceso, incluye la manera formal de la presentación, la especialización y las calificaciones del perito. Contempla la credibilidad de los procesos empleados para producir la evidencia que se está presentando ante quien juzga.

3.8.1. Centro de Recopilación, Análisis y Difusión de Información Criminal (CRADIC)

La relación del Centro de Recopilación, Análisis y Difusión de información criminal en Guatemala es importante con la evidencia digital, ya que es una institución “Bajo la Subdirección General de Investigación Criminal, el CRADIC realiza análisis intercomunicacional sobre personas sospechosas de un delito. Recientemente se le ubica como la oficina de inteligencia policial… la parte de la Inteligencia referida a las actividades criminales específicas que, por su naturaleza, magnitud, consecuencias previsibles, peligrosidad o modalidades, afectan la libertad, la vida, el patrimonio de los habitantes, sus derechos y garantías y las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional”.[56] Tiene a su cargo realizar la investigación criminal de carácter preventiva en Guatemala, para el efectivo cumplimiento de sus actividades recopila y analiza la información de personas sospechosas en la comisión o posible participación en hechos delictivos,

[56] Dabroy, Jahir. *La importancia de la labor de inteligencia criminal en Guatemala*. Guatemala. RESDAL. 2009. Pág. 5. Disponibilidad y acceso: http://www.resdal.org/jovenes/inteligencia-criminal-dabroy1.pdf. fecha de consulta: 02.10.2016.

esto implica que el Centro de Recopilación, Análisis y Difusión de información criminal debe saber manejar indicios digitales a través de procedimientos eficaces y funcionales para garantizar una información, datos e inclusive archivos relevante para la investigación criminal, sin desplazar de las principales funciones al Ministerio Público y la labor que realiza el Instituto Nacional de Ciencias Forenses de Guatemala.

En consecuencia, la recolección y aseguramiento de la evidencia digital sienta sus bases en el manejo adecuado de la cadena de custodia la cual debe ser garantizada como parte de una investigación criminal objetiva, esto implica que desde el momento en que se secuestran los dispositivos de tecnología, atraviesan la fase de identificación, recuperación y consolidación de datos, archivos e información sospechosa en la comisión de un hecho delictivo, consecutivamente la extracción, transporte, entrega y análisis de la evidencia se debe procurar tener un estricto control sobre quienes acceden a la información o la manipulan de diversas formas, ya que como parte de las características más significativas esta puede ser borrada o alterada de forma fácil, por lo que la cadena de custodia implica un resguardo y cuidado especial sobre la evidencia digital ya que su utilidad es determinante en la absolución o condena del acusado de la comisión de un hecho delictivo.

CAPÍTULO IV

MANEJO DE LA CADENA DE CUSTODIA EN LA RECOLECCIÓN DE EVIDENCIA DIGITAL

4.1. Generalidades

La evidencia digital y la cadena de custodia constituyen uno de las principales figuras en la actualidad en la ciencia de la investigación criminal, ya que la influencia de la tecnología ha contribuido de forma negativa en la efectiva realidad del delito. Es importante mencionar que son múltiples los usos de la evidencia digital en el ámbito probatorio y por esa influencia extensa de la tecnología la mayoría de delitos que acontecen en la actualidad de una u otra manera necesitan del auxilio de algún dispositivo de tecnología; esta representa una garantía en la investigación criminal de carácter digital ya que se encuentra presente en muchos procesos penales que son de importante coyuntura a nivel guatemalteco, por lo que considerar un adecuado manejo de la cadena de custodia en la recolección de evidencia digital debe observar parámetros importantes que son generales en la investigación criminal y que son de aplicación uniforme para indicios o evidencias de distinta naturaleza. Por lo que resulta practico considerar la objetividad, autenticidad, legalidad, idoneidad, inalterabilidad y documentación de los indicios digitales con la mera finalidad de crear una cadena de custodia digital adecuada.

La información y los sujetos de investigación en los delitos informáticos especialmente deben ser individualizados de forma correcta, es decir que existen diferentes figuras criminales que se relacionan con la evidencia digital y su respectiva recolección como lo son delitos financieros, falsificaciones, piratería de software, asuntos de propiedad intelectual, intromisión en redes, la violación a la privacidad, clonación de información financiera, robo de identidad, fraude de telecomunicaciones, pornografía y abusos infantiles son algunos de los delitos en los que por lo general se utiliza un medio de tecnología para su comisión, sin embargo en delitos de extorsión, homicidio, estada o asesinatos también es posible que se

hayan consumado con el auxilio de un dispositivo de tecnología del cual se desprende evidencia digital que debe ser sometida a investigación criminal y consecuentemente debe hacerse efectiva una cadena de custodia digital técnica. En consecuencia, la cadena de custodia debe observar los principios del peritaje pudiéndose indicar los siguientes:

a) Objetividad: es uno de los principios fundamentales que debe orientan la investigación criminal, se consagra a nivel legal como rector en la función del Ministerio Público como ente titular de la investigación en Guatemala; por lo que la recolección de evidencia digital y la conformación de una cadena de custodia digital debe estar revestida de imparcialidad por parte del perito y debe observar la ética en sus funciones para actuar con independencia, evitando así la alteración culposa y dolosa de la información digital lo que influiría significativamente en el resultado del proceso penal.

b) Autenticidad: uno de los problemas que se presentan en la investigación criminal es la determinación de la autenticidad de la información digital, ya que atendiendo a su principal característica que es fácilmente duplicable y es complejo determinar si es el archivo original o es un duplicado es necesario que se documente e identifique el indicio o evidencia digital, esto implicaría la descripción integra del mismo que se está recolectando para lo cual la consignación de la hora y fecha son trascendentales para identificar cualquier alteración o modificación de la información, datos, archivos y programas que sean sometidos a investigación, esto implica la acreditación de la autenticidad al transformarse en un medio de prueba que se pretende integrar al proceso penal guatemalteco.

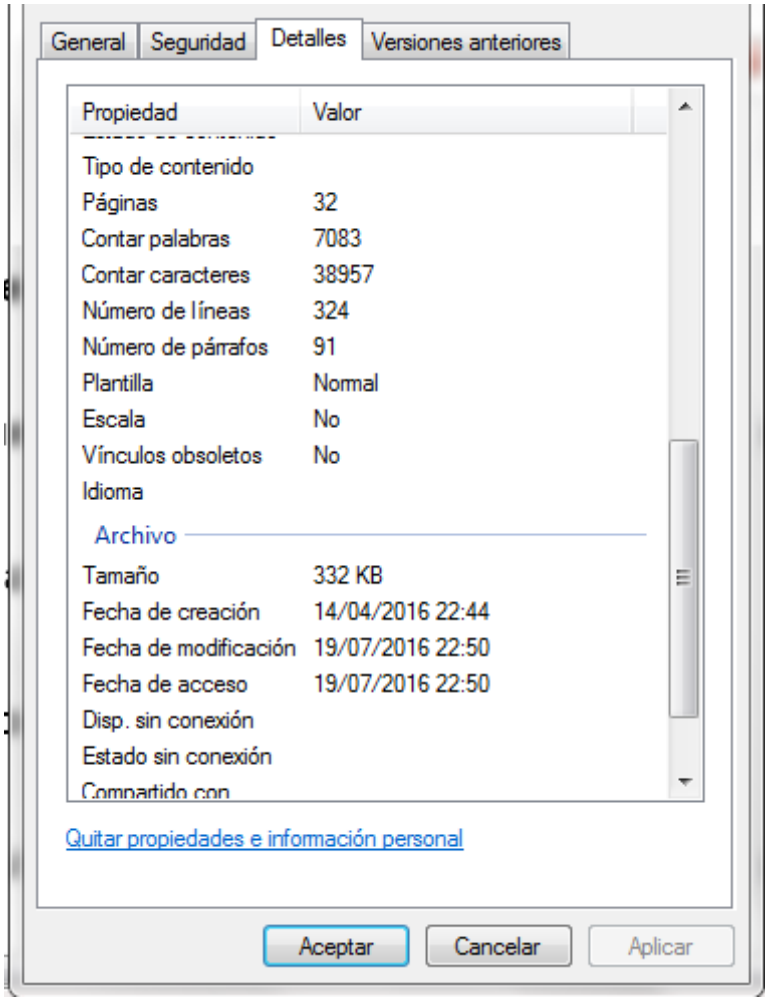
c) Legalidad: la legalidad va de la mano con la investigación criminal, para su efecto el perito orientado a la recolección de evidencia digital debe conocer la legislación que rige la actividad pericial y debe cerciorarse que se cumple a cabalidad con los requisitos exigidos por la ley para obtener información, datos, archivos, registros y software digital para su investigación; esto implica que tal como sucede con la

investigación criminal tradicional el perito en informática forense debe contar con las resoluciones legales que acrediten la intervención en la privacidad de las personas, en este caso del sindicado considerando que toda la información digital que este ha producido se encuentra normada en leyes ordinarias y en la propia Constitución Política de la República de Guatemala que indican que para someterla a investigación criminal debe mediar resolución judicial que la autorice, caso contrario se corre el riesgo en caer en ilegalidad o ilicitud de la evidencia digital la cual en este caso resultaría inútil e ineficaz al momento de integrarse al proceso penal ya que no reuniría los requisitos de ley.

d) Idoneidad: El termino idóneo hace referencia en investigación criminal a las condiciones necesarias para demostrar la comisión de un delito que se ha imputado por el ente investigador a un determinado sujeto, esto lleva implícito que el perito en informática forense debe considerar que los medios de prueba al momento de integrarse al proceso penal deben ser suficientes y relevantes para el caso que se está dilucidando, por lo que la idoneidad de los medios de prueba digitales empieza conjuntamente con la recolección de indicios o evidencia digital que pueda considerarse durante la investigación criminal.

e) Inalterabilidad o integridad de la evidencia digital: este principio es indispensable especialmente cuando se habla de indicios o evidencias digitales, al considerar lo frágil de los datos e información producida con los distintos dispositivos de tecnología, resulta imperativo que se considere la integridad de la información obtenida de estos; caso contrario no existiría objetividad por parte del perito y especialmente en casos de evidencia digital se podría incurrir en serias responsabilidades administrativas e inclusive penales, ya que la evidencia y la prueba deben ser las mismas que se han obtenido en la escena considerada del crimen con las que se aportan al proceso penal guatemalteco, por lo que garantizar la inalterabilidad de la información digital es el reflejo de una adecuada cadena de custodia digital y su técnico manejo.

f) Documentación: los indicios digitales y la evidencia que sea originada en dispositivos de tecnología que va ser sometida a investigación criminal debe ser documentada y debe ser descrita de forma íntegra especialmente reuniendo la información de fecha y hora de creación, ya que esta información en su momento puede indicar si esta fue alterada o no lo que implicaría un giro totalmente distinto en el ejercicio de la actividad punitiva y la investigación criminal, esto conlleva la descripción integra de los pasos que se han desarrollado para la recolección y manejo de la cadena de custodia incluyendo los sujetos que han intervenido en la misma, ejemplo:



Fuente: realizado por el investigador

4.2. Riesgos de la cadena de custodia digital

La cadena de custodia sin duda alguna es muy importante en la investigación criminal en la actualidad, ya que esta representa en los medios informáticos la certeza de la objetividad y legalidad de los nuevos medios de prueba que se implementan en el proceso penal guatemalteco, cabe resaltar que aunque resultar ser un tema novedoso es posible identificar riesgos que son subyacentes a las prácticas avanzadas de informática, es decir el hacking y la intromisión remota por parte de sujetos especializados representa un riesgo para la alteración de la cadena de custodia digital en especial cuando esta es ingresada a un dispositivo de tecnología para su análisis; es necesario plantear algunos ejemplos que resultan ser posibles y representa un peligro para la cadena de custodia digital.

- El primer planteamiento que establece el investigador es la capacidad técnica y especializada para el manejo de la cadena de custodia digital, esto implica que el perito debe tener los conocimientos necesarios en informática y no solamente información básica respecto a lo delicado de la información, datos, registros, archivos y software digital; por lo que representa un riesgo para la cadena de custodia digital la negligencia, imprudencia e impericia de los sujetos que manipulan los dispositivos, partiendo de la premisa importante que se desprende de la amplia esfera de la informática y los diversos sistemas operativos que existen en la actualidad, por lo que no es suficiente que el perito en informática forense conozca de forma básica la esfera de la computación y posea una acreditación institucional, ya que la certificación en informática forense debe observar los parámetros internacionales.

- El segundo planteamiento radica en la seguridad informática que posean los dispositivos en los cuales se pretende realizar el análisis de la información recolectada y sometida a investigación criminal. Los avances tecnológicos han permitido el desarrollo de nuevas herramientas de hacking que permiten la infiltración por parte de individuos denominados hackers, los cuales básicamente tienen la capacidad intelectual y técnica para acceder de forma remota a cualquier

dispositivo de tecnología con diferentes fines, ya sea desde robar información personal, alterar evidencia digital o suprimir las bases de datos existentes; este quizás es uno de los riesgos más importantes ya que los grandes gobiernos, instituciones gubernamentales, financieras e inclusive agencias de investigación criminal internacional como CIA, DEA y FBI, entre otras han sido expuestos por errores de seguridad que han sido aprovechados por hackers y que han sido expuesto a la prensa internacional así como a otros interesados, esto no es más que la certeza de los riesgos que se presentan frente a la cadena de custodia digital, por lo que considerar que es inalterable media vez ha sido recolectada no es correcto ya que se presentan circunstancias técnicas del perito que pueden afectar la cadena de custodia así como de otros sujetos que intervienen o simplemente puede ser afectada por un error de seguridad que permita la infiltración de agentes externos con un propósito definido.

4.3. Fundamentación legal de la cadena de custodia digital

Es indispensable considerar que la investigación criminal es una actividad o procedimiento que se ha delegado por mandato legal al Ministerio Público quien conjuntamente con instituciones como el Instituto Nacional de Ciencias Forenses, la Comisión Internacional Contra la Impunidad en Guatemala y el Centro de Recopilación, Análisis y Difusión de Información Criminal, entre otras. Poseen un respaldo de carácter jurídico legal que los faculta para desarrollar sus procedimientos de investigación criminal específicos; en este sentido la cadena de custodia digital debe poseer una fundamentación normativa cumpliendo con el principio de legalidad que forma parte del proceso penal y de la investigación criminal, sin embargo como parte de libertad probatoria así como de la influencia de la tecnología en la investigación criminal y en el derecho penal se ha implementado la cadena de custodia digital de forma atípica, ya que no se encuentra regulada en la ley y su viabilidad deviene de la mera libertad probatoria; por lo que resulta importante considerar que en materia de investigación criminal aunque no se encuentre regulada la cadena de custodia digital en procedimientos institucionales o manuales de investigación criminal en Guatemala, se debe de regular con la mera finalidad de

crear procedimientos uniformes y disponer los principios rectores que deben guiar esta forma de investigación criminal, esto con la intención de brindar una certeza jurídica sobre la actividad de investigación criminal en el campo de la informática y la computación, esto responde también a las responsabilidades civiles y penales que se pudieran derivar como consecuencia de la impericia, negligencia o imprudencia de la manipulación de información o datos digitales, así como en los casos de alteración o supresión de información de forma dolosa que pueda implicar de forma conveniente la condena o absolución de un procesado por delitos que se relacionan con dispositivos de tecnología. El director de la dirección de análisis criminal hace referencia que "no existe",[57] un reglamento o disposición legal que recaiga específicamente sobre la evidencia digital y su respectiva cadena de custodia, por lo que en consecuencia, es necesario aplicar por defecto las disposiciones contenidas en el manual de normas y procedimientos para el procesamiento de la escena del crimen del Ministerio Público acuerdo 166-2013, sin embargo estas no son suficientes para tratar el contenido de la evidencia digital y su respectiva cadena de custodia ya que los procedimientos uniformes aplicados a la evidencia física presentan características como la tangibilidad que no aplica para la evidencia digital.

4.4. Requisitos para el manejo de la cadena de custodia en la recolección de evidencia digital

En el contexto de investigación criminal en Guatemala existe una serie de disposiciones contenida en el Manual de Investigación Criminal del Ministerio Público para el manejo de la cadena de custodia, sin embargo en la esfera digital no se cuenta con una disposición concreta y desarrollada frente a estos nuevos medios de investigación criminal que resulta muy importantes en la actualidad para la averiguación de la verdad; por su parte el ingeniero Carlos Rodríguez Jefe de la subdirección de criminalística operativa al ser consultado respecto al procedimiento y los requisitos para el manejo de la cadena de custodia en la recolección de evidencia

[57] Director de la dirección de análisis criminal. *Entrevista trabajo de campo: Manejo de la cadena de custodia en la recolección de evidencia digital*. Guatemala. 2016.

ha referido únicamente que “es confidencial”[58] el procedimiento lo que es considerado por el investigador incorrecto al negar tan importante información, ya que como servidor público deben existir parámetros generales que contribuyan en la formación de profesionales en la investigación criminal y que a su vez permita desarrollar de forma especializada lo que es la cadena de custodia de la evidencia digital. Como parte de una investigación objetiva es necesario observar algunos criterios internacionales que aunque no son vinculantes suponen una estructura ordenada y sistematizada de requisitos para el manejo de la cadena de custodia de la evidencia digital. Para el efecto se propone las normas ISO 27037 para la identificación, recolección, adquisición y preservación de la evidencia digital.

4.5. Identificación, recolección, adquisición y preservación de la evidencia digital Norma ISO 27037

Contenida en siete capítulos la Norma de la Organización Internacional para la Normalización es una importante guía para el tratamiento de la evidencia digital, aunque dicha norma no es vinculante para los Estados y las instituciones que tienen la competencia de desarrollar la investigación criminal, sin embargo supone un importante instrumento para los investigadores particulares y cualquier profesional en formación que se interese por la evidencia digital y su manejo, dicha norma se desarrolla en la siguiente estructura:

1. Alcance
2. Marco de referencia
3. Términos y definiciones
4. Abreviaturas
5. Descripciones generales
6. Elementos para la Identificación, recolección, adquisición y preservación de Evidencia Digital
7. Instancias en la Identificación, recolección, adquisición y preservación de Evidencia Digital

[58] Rodríguez, Carlos. *Entrevista trabajo de campo: Manejo de la cadena de custodia en la recolección de evidencia digital*. Guatemala. Jefe de la subdirección criminalística operativa DICRI. 2016.

Gervilla Rivas plantea las generalidades relacionadas a la norma ISO 27037 consistente en la identificación, recolección, adquisición y preservación de la evidencia digital. Indica que "Dentro de la seguridad informática cabe destacar una normativa ampliamente conocida, es la familia ISO 27000. Esta serie de normas son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). Esta serie contiene diversas normas todas relacionadas con las mejores prácticas recomendadas en Seguridad de la Información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). Concretamente, existe una norma dedicada en exclusiva al análisis forense, se trata de la ISO 27037 Directrices para la identificación, recolección, adquisición y preservación de la prueba digital. Esta norma ofrece orientación para tratar situaciones frecuentes durante todo el proceso de tratamiento de las pruebas digitales. Además define dos roles especialistas:

- DEFR (Digital Evidence First Responders): Expertos en primera intervención de evidencias electrónicas.
- DES (Digital Evidence Specialists): Experto en gestión de evidencias electrónicas.

ISO 27037 proporciona orientación para los siguientes dispositivos y circunstancias:

- Medios de almacenamiento digitales utilizados en equipos varios como por ejemplo discos duros, disquetes, discos magneto-ópticos y ópticos y otros similares.
- Teléfonos móviles, PDAs, tarjetas de memoria.
- Sistemas de navegación móvil (GPS).
- Cámaras de video y cámaras digitales (incluyendo circuitos cerrados de televisión).
- Ordenadores estándares con conexiones a redes.
- Redes basadas en protocolos TCP/IP y otros protocolos digitales.
- Otros dispositivos con funcionalidades similares a las descritas anteriormente".[59]

[59] Gervilla Rivas, Carles. *Metodología para un análisis forense*. España. Universitat Oberta de Catalunya. España. 2014. Pág. 19, 20.

Esta norma supone criterios orientadores sobre el manejo de la evidencia digital, son parte de la Organización Internacional para la Estandarización y son realmente importantes en la investigación forense ya que desarrolla los aspectos más relevantes de los especialistas en la investigación forense de evidencias digitales, plantea un experto de primera intervención quien tiene a su cargo la recolección de evidencias digitales y el segundo experto en gestión de evidencias electrónicas se encarga de realizar el peritaje respectivo en relación al delito investigado, además señala el autor que la ISO 27037 proporciona una amplia orientación en dispositivos de tecnología en los cuales es posible que se genere evidencia digital, partiendo desde los medios de almacenamiento digital de datos que pueden ser fijos, temporales, externos, internos, entre otros, según sus propias características; además aborda aspectos relacionados a los teléfonos móviles incluye desde los más tradicionales hasta los de la más alta tecnología, así como los archivos de registro que genera y otros dispositivos portátiles como PDAs.

En cuanto a computadores y ordenadores portátiles conjuntamente con su transferencia de datos vía redes informáticas plantea un amplio contexto en los diversos sistemas operativos que son funcionales con estos, además desarrolla consideraciones relacionadas al sistema de posicionamiento global (GPS), video vigilancia y cualesquiera otros archivos que puedan almacenarse en cámaras de video, cámaras digitales e inclusive dispositivos similares multifuncionales. En cuanto a las redes basadas en protocolos TCP/IP y otros protocolos digitales es importante resaltar que se vuelve una labor aún más compleja porque la investigación criminal debe seguir rastros minuciosos que pueden ser fácilmente ocultos, por lo que la aplicar la informática forense a redes basadas en distintos protocolos digitales implica una labor sobre especializada y muy delicada para identificar potencialmente la evidencia digital en especial cuando se han cometido delitos a través de direcciones de protocolo privadas o VPN conocidas en el mercado. Esta norma crea bases orientadoras sobre la identificación, recolección, recepción, adquisición, manejo, protección y preservación de las evidencias forenses digitales; implica toda aquella información que por su naturaleza posteriormente puede ser útil dentro de un

proceso penal debidamente instruido en auxilio de la tecnología en cuanto a los medios de prueba. No poseen carácter vinculante para la investigación criminal sino más bien implican normas estandarizadas para promover métodos adecuados y procesos para la recolección y cadena de custodia de las evidencias digitales.

Uno de los principales problemas que enfrenta la cadena de custodia y el manejo de la evidencia digital es la ausencia de uniformidad de los procedimientos de investigación criminal, el ingeniero Carlos Rodríguez refiere que el manejo de la cadena de custodia y procedimientos para la recolección de la evidencia electrónica "Se desarrolla a través del seguimiento del manual y procedimientos para el procesamiento de la escena de crimen",[60] sin embargo tal como se ha planteado en la presente investigación la esfera de la informática y la computación es tan amplia que necesita en el caso de este nuevo medio de investigación criminal procedimientos preestablecidos y específicos para evitar errores que puedan perjudicar la averiguación de la verdad. Por lo que la adopción de enfoques similares en la investigación criminal solamente recae a los aspectos teóricos ya que en la práctica es necesario considerar la especialización del perito en determinadas áreas de la informática y la computación que son producto de estudios prolongados que inclusive en Guatemala no existen en la actualidad, esto implica métodos, proceso y controles funcionales que deben ser adoptados por el Manual de investigación criminal del Ministerio Público guatemalteco

4.5.1. Tratamiento de la evidencia digital según ISO 27037

Para establecer el tratamiento de la evidencia digital es indispensable observar los distintos parámetros que convergen en su contenido conjuntamente con los aportes que han realizado algunos profesionales en el Congreso Argentino de Ingeniería Forense en el año dos mil catorce. Para desarrollar el tratamiento de la evidencia digital partiendo de lo que dispone la norma ISO 27037 es importante comprender que el problema critico en la investigación forense es la adquisición y conservación

[60] Rodríguez, Carlos. *Entrevista trabajo de campo: Manejo de la cadena de custodia en la recolección de evidencia digital*. Guatemala. Jefe de la subdirección criminalística operativa DICRI. 2016.

para garantizar la integridad de los datos digitales que se hayan obtenido, al igual que con la evidencia física convencional, es crucial para la primera y subsiguientes diligencias contar con especialistas de la evidencia digital para mantener la cadena de custodia de todas las pruebas forenses digitales, asegurando que se recoge y sea protegida a través de procesos estructurados que sean aceptables para los tribunales, este último aspecto es relevante en la objetividad con la que actúa el ente investigador y los parámetros aceptados por los jueces en cuanto a la evidencia digital. La manipulación incorrecta de la información y datos obtenidos puede ser fácilmente dañada o alterada debido a una manipulación incorrecta ya sea de forma accidental, por lo que se requieren niveles de referencia que sean definidos dentro de los procesos de recolección y preservación a través de una cadena de custodia adecuada.

4.5.1.1. Alcance de la norma ISO 27037:

Este estándar provee lineamientos para el manejo de Evidencia Digital y establece las siguientes actividades: identificación, recolección, adquisición y preservación de Almacenamiento digital.

1. Dispositivos móviles
2. GPS (Sistema de posicionamiento global)
3. CCTV (circuito cerrado de televisión)
4. Dispositivos en red TCP/IP o similar

Incluye cualquier otro dispositivo en cualquier forma que puedan ser considerados como fuentes de evidencia digital.

En cuanto a los requerimientos de la evidencia digital cabe resaltar tres importantes para las Normas ISO 27037 los cuales son relevancia, confiabilidad y suficiencia, son desarrollados por el ingeniero Gustavo Daniel Presman en el marco del Primer Congreso Argentino de Ingeniería Forense de la manera siguiente:

- “Relevancia: Este es un concepto jurídico que indica que la evidencia digital debe estar relacionada con los hechos investigados.

- Confiabilidad: La evidencia debe ser confiable por lo que debe ser repetible y auditable por un tercero que usando el mismo principio de operación aplicado llegue a idénticos resultados.
- Suficiencia: La evidencia recolectada debe ser suficiente para sustentar los hallazgos obtenidos por el analista forense, es lo que denomino recolección efectiva".[61]

Estos tres requerimientos se justifican a partir de la necesidad de la prueba dentro de un proceso debidamente instruido, por lo que al considerar la relevancia de la evidencia digital se relaciona con la pertinencia de la misma y si realmente los datos o información que se están tratando son los que efectivamente pueden demostrar la comisión de un delito. En cuanto a la confiabilidad es un criterio importante que refiere que la evidencia digital debe ser auditable por un tercer que va de la mano con el principio de contradicción de la evidencia al momento de transformarse en prueba, tal como lo plantea Presman la posibilidad de poderse auditar por un tercer genera la confianza al momento de valorar la prueba por el tribunal considerando que al ser repetible el procedimiento de investigación se llegaría al mismo resultado, caso contrario se puede considerar que la prueba ha sido alterada. En cuando a la recolección efectiva o denominada bajo la consideración de suficiente, es necesario que en observancia del principio de objetividad que debe revestir al investigador criminal esta debe ser suficiente para sustentar la averiguación de la verdad ya sea para lograr una condena o una absolución mediante la labor objetiva.

4.5.1.2. Consideraciones sobre la cadena de custodia digital según ISO 27037.

La norma ISO 27037 plantea unas consideraciones importantes para el manejo de la cadena de custodia sobre la evidencia digital, resultando necesario cumplir las recomendaciones siguientes:

[61] Presman, Gustavo Daniel. *ISO/IEC 27037: normalizando la práctica forense informática*. Argentina. 1er Congreso Argentino de Ingeniería Forense. 2014. Pág. 8. Disponibilidad y acceso: http://docplayer.es/5605332-Iso-iec-27037-normalizando-la-practica-forense-informatica.html fecha de consulta: 20.11.2016.

- “Minimizar el manejo de la evidencia digital original.
- Documentar cualquier acción que implique un cambio irreversible.
- Adherirse a las regulaciones y leyes locales.
- No extralimitarse en sus funciones”.[62]

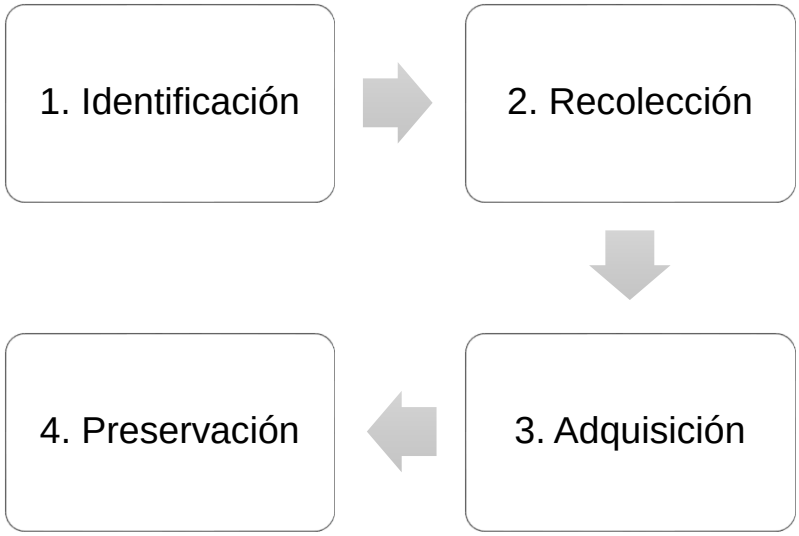
Desde un punto de vista general, estas recomendaciones son importantes en cuanto a la evidencia digital ya que por sus propias características esta es susceptible a sufrir cambios irreversibles para los cuales es necesario generar una documentación adecuada y descriptiva lo más amplio, sin embargo es importante resaltar que se recomienda minimizar el manejo de la evidencia digital original, ya que desde que se identifica se pretende manejar una cadena de custodia digital lo más prudente para que no se generen problemas respecto a la confiabilidad de esta, bajo la recomendación de adhesión a leyes y regulaciones locales cabe señalar que en Guatemala se implementa el Manual de investigación criminal del Ministerio Público, sin embargo frente a una evidencia tan compleja como lo es la que se produce en dispositivos de tecnología resulta importante que de forma progresiva se desarrollen procedimientos exclusivos para el manejo y preservación de los indicios o evidencias digitales. La extralimitación de las funciones recae especialmente en el respeto a la privacidad como un derecho constitucional, esto implica que toda la información y datos digitales que se han recopilado para una investigación criminal deben permanecer bajo estricta confidencialidad para no afectar derechos protegidos por la Constitución Política y otras leyes.

Presman refiere que el proceso de estandarización o normalización del manejo y preservación de la evidencia digital, así como la cadena de custodia debe observar importantes procedimientos, los cuales garantizan la eficacia de la evidencia al transformarse en prueba que se integrará eventualmente al proceso penal y para el efecto propone cuatro etapas relevantes para el resguardo de la evidencia digital.

1. **“Identificación**: es el reconocimiento de donde se halla la evidencia digital, sea esta lógica.

[62] *Ibíd.* pág. 9.

2. **Recolección**: frecuentemente el DEFR (individuo autorizado, entrenado y calificado para actuar en la escena del hecho con capacidad de recolección y adquisición de evidencia digital) deberá tomar la decisión de recolectar la evidencia y trasladarla al laboratorio para su adquisición, en función del tiempo y los recursos informáticos disponibles en la escena del hecho, sustentado por el mandato judicial. En cualquier caso, deberá documentar su decisión fundamentándola y estará preparado para defenderla en una corte.
3. **Adquisición**: es el proceso de copia forense que el DEFR o DES realizará obteniendo una copia binaria exacta del contenido lógico o físico de los objetos involucrados en la investigación. La norma establece que la copia debe ser verificada con un "método de verificación probado" evitando expresarse sobre la utilización de algún HASH en particular.
4. **Preservación**: la evidencia digital deberá ser preservada para asegurar su integridad durante todo el proceso. Esto incluye el embalaje, que en algunos casos tiene requerimientos especiales".[63]



Fuente: realizado por el investigador

Para la norma ISO 27037 darle cumplimiento a este procedimiento es fundamental para asegurar la adecuada preservación y recolección de la evidencia digital, por lo

[63] *Ibíd.* Pág. 10, 11.

que para identificar los indicios electrónicos y la evidencia digital es necesario hacer un reconocimiento preliminar para establecer los procedimientos para llevar a cabo en cuanto a la sustracción de la información digital, en cuanto a la recolección refiere Presman que debe ser un individuo autorizado, entrenado y calificado para actuar en la escena del hecho con capacidad de recolección y adquisición de evidencia digital, para el efecto resulta necesario que fundamente sus decisiones las cuales debe defender en los juzgados al momento de la presentación de la información obtenida. En cuanto a la adquisición y preservación son procesos más complejos ya que consiste en la copia binaria del contenido, por lo que se debe utilizar métodos verificados por la legislación local para que tengan su respectiva validez y por último se establece el embalaje que constituye un requerimiento especial por la naturaleza de la evidencia, esto con la mera finalidad de salvaguardar la integridad durante todo el proceso de investigación criminal.

En consecuencia, refiere el ingeniero Presman que para la ISO 27037 la cadena de custodia de la evidencia digital debe llenar los requisitos siguientes además de los que refieren las normas locales y leyes procedimentales que rigen la investigación criminal:

Considerando que la cadena de custodia constituye el "registro de identificación cronológica del movimiento y manejo de evidencia potencial. Puede ser un formulario o un conjunto de documentos conteniendo como mínimo:

1. Un identificador único de evidencia.
2. Quien accedió a la evidencia, en qué lugar/fecha/hora.
3. Quien retiró o almacenó la evidencia del lugar de resguardo.
4. Motivo sustentable de autoridad relevante.
5. En caso de producir cambios en la evidencia. Quien los hizo y su justificación".[64]

La cadena de custodia constituye un estricto control que se relaciona al movimiento cronológico y manejo de la evidencia digital recuperada, por lo general se realiza de

[64] *Ibíd.* Pág. 13.

forma documental pero es posible realizarse por dispositivos de tecnología que preservan la información y datos digitales recuperados; sin embargo es fundamental identificar e individualizar la evidencia de forma adecuada atendiendo a sus características y múltiples formatos; así como también tener un minucioso control sobre quien accedió a la evidencia y quien la retiro consignando lugar, fecha y hora según norma ISO 27037.

La cadena de custodia de la evidencia digital y su manejo se deben hacer acorde a las normativas locales, sin embargo se ha intentado establecer procedimientos uniformes que orienten a los investigadores en tan compleja labor, ya que la investigación criminal tradicional no plantea las herramientas y métodos necesarios en cuanto a la esfera digital o electrónica; por lo que es necesario un apoyo metodológico para proporcionar una adecuada gestión de la evidencia digital en Guatemala, en este sentido se ha convertido en una labor importante la informática forense en la actualidad por los múltiples dispositivos y sistemas operativos que existen en el mercado son fuente generadora de evidencia de relevancia en las nuevas modalidades para delinquir, por el contrario frente a la ausencia de una normativa especializada y procedimientos uniformes o estandarizados existe un gran margen de potenciales errores que surgen dentro de la cadena de custodia de la evidencia digital, en cuanto a l norma ISO 27037 es indispensable seguir sus recomendaciones ya que aunque no son vinculantes son una importante guía para los investigadores forenses en materia de informática.

Cuadro comparativo cadena de custodia digital

Indicador	Guatemala	Colombia
Regulación legal	No tiene de forma subsidiaria el Código procesal penal guatemalteco y Manual de normas y procedimientos para el procesamiento de la escena del crimen del Ministerio Público.	Guía No. 13: sobre seguridad y privacidad de la información que se centra en la evidencia digital.
Secuestro de dispositivo	**Artículo 200** del Código Procesal Penal bajo el nombre de Orden de secuestro el cual indica que "La orden de secuestro será expedida por el juez ante quien penda el procedimiento o por el presidente, si se tratare de un tribunal colegiado. En caso de peligro por la demora, también podrá ordenar el secuestro el Ministerio Público, pero deberá solicitar la autorización judicial inmediatamente, consignando las cosas o documentos ante el tribunal competente. Las cosas o documentos serán devueltos, si el tribunal no autoriza su secuestro"	**Artículo 92: medidas cautelares sobre bienes del Código de Procedimiento penal colombiano**: el juez de control de garantías, en la audiencia de formulación de la imputación o con posterioridad a ella, a petición del fiscal o de las víctimas directas podrá decretar sobre bienes del imputado o del acusado las medidas cautelares necesarias para proteger el derecho a la indemnización de los perjuicios causados con el delito.
Creación bitácora	el formato o formatos dentro de los cuales deberán anotarse los nombres y firmas de los servidores públicos que de manera sucesiva intervengan en la cadena de custodia, desde que se hallan los indicios hasta el final del proceso. Además se debe anotar la fecha y hora de entrega y recepción del indicio, la descripción de los objetos o indicios, sus características físicas, color, peso, etcétera, el lugar de los hechos o del hallazgo Y todos los datos que se consideren relevantes para la averiguación previa	**Instrucción 11.1:** En la creación y aseguramiento de un documento, ya sea físico o electrónico, que permita llevar un historial de todas las actividades que se llevan a cabo durante el proceso, y de los hallazgos encontrados, de modo que se tenga un resumen que permita hacer la reconstrucción del caso tiempo después de que este haya sido analizado"
Identificación y detección	En Guatemala no se tiene un procedimiento uniforme, por lo que se utiliza de forma subsidiaria Manual de	**Instrucción 11.7:** "La identificación de las particiones en un dispositivo es de vital

de indicios o evidencia digital	normas y procedimientos para el procesamiento de la escena del crimen, así como se utiliza el criterio del perito para determinar el procedimiento adecuado, por lo que no se garantiza el fundamento jurídico.	importancia, ya que reconocerlas implica la identificación de su sistema de archivos, mediante el cual se pueden reconocer características especiales de la organización de la información y se puede definir la estrategia de recuperación de archivos adecuada.
Recolección de indicios digitales	A nivel jurídico y procedimental en Guatemala no se cuenta con una instrucción que haga referencia a la técnica adecuada de los indicios digitales en general, sin embargo, se utiliza el dispositivo UFED para realizar la diligencia.	**Instrucción 11.22**: El analista forense deberá trabajar junto con el equipo de incidentes, para decidir la manera adecuada de contener el incidente permitiendo a su vez recolectar la mayor cantidad de información posible (siempre y cuando sea posible
Transporte y entrega de la evidencia digital	El transporte se realiza por los fiscales a cargo de la escena del crimen, trasladando para el efecto al Instituto Nacional de Ciencias Forenses a través de la fiscalía correspondiente para el análisis.	En Colombia se aplica el procedimiento predeterminado para el aseguramiento de la evidencia, con la diferencia que se entrega en centros especializados para su análisis.
Análisis de la evidencia digital	A nivel guatemalteco no existe un procedimiento uniforme para analizar la evidencia digital o al menos un manual específico para esta ardua labor, por lo que se carecen de principios legales y procedimentales para su análisis.	**Instrucción 12:** En esta fase se realizará un análisis de la información que logró extraerse de las diferentes fuentes y que se considera relevante o prioritaria para ser estudiada (después de realizar la depuración en las fases anteriores).
Reporte de evidencia digital	En Guatemala no existe manual que indique la forma de presentación del reporte y los requisitos que debe llenar conjuntamente con las conclusiones.	**Instrucción 13:** La fase final del procedimiento de evidencia digital es el reporte, el cuál presenta toda la información y la evidencia obtenida en la fase de análisis.

CAPÍTULO V

ANÁLISIS Y DISCUSIÓN DE RESULTADOS

La evidencia digital abarca cualquier tipo de información, datos, registros, archivos, formatos y extensiones que se originan en dispositivos de tecnología; esta implica una extensa gama de formas de reproducción y los sistemas operativos en las cuales se pueden encontrar presentan verdaderos retos para los investigadores criminales especializados en informática forense. Sus principales características es el anonimato, volatilidad y sobre todo la facilidad para duplicar de forma idéntica la evidencia digital original siendo casi imposible distinguir cual es la original, por lo que más allá de ser un elemento de investigación preciso presenta obstáculos que solamente pueden ser superados por la preparación profesional y especializada de forense en informática. Por lo que la evidencia digital supone un medio de investigación criminal novedoso en la esfera guatemalteca, ya que no solo difiere de los procedimientos tradicionales de investigación criminal sino que implica una compleja estructura de dispositivos y herramientas digitales para el respectivo análisis de los datos e información considerada útil en la averiguación de la verdad respecto a un delito.

Una adecuada manera del manejo de la cadena de custodia es observar los lineamientos generales establecidos por las instituciones guatemaltecas encargadas de desarrollar la investigación criminal, sin embargo es indispensable tomar en cuenta que cuando se pretende manipular información o datos digitales estos son fácilmente alterados ya sea de forma voluntaria o involuntaria, lo que implica que se debe ser extremadamente cauteloso en la forma en que se pretende manipular la información; en este sentido el adecuado manejo de la cadena de custodia de la evidencia digital implica que se debe mantener un registro documental o una bitácora respecto a los agentes o sujetos que han tenido interacción con la información al momento de identificarla, ya que es importante minimizar e inclusive eliminar la

interferencia de agentes exteriores que pudieran afectar la esencia de la evidencia digital y no cumpla con los requisitos de admisibilidad en el proceso penal.

La cadena de custodia de la evidencia digital resulta importante para preservar la confiabilidad y autenticidad de los datos e información que son considerados importantes para la investigación criminal, sin embargo hay que considerar circunstancias tan básicas que revisten de seguridad a la cadena de custodia más alá de la información específica y detallada de lo identificado, de quienes han tenido contacto con las evidencias y la manera fundamentada en que se realizará el procedimiento de recolección de la evidencia o indicios digitales.

Es por ello que el buen manejo de la cadena de custodia de la evidencia digital permite la admisibilidad de las pruebas en el juicio de reproche, siempre teniendo en cuenta la volatilidad de la evidencia digital que implica que esta puede ser destruida o modificada con facilidad y por fuerzas exteriores, en este sentido la seguridad informática actúa como repelente de los ataques remotos que pretendieran en algún momento alterar información digital sujeta a investigación.

Se plantea la siguiente cadena de custodia como propuesta novedosa en los entes encargados de la recolección de evidencia en Guatemala:

1. Secuestro de los dispositivos de tecnología o aquellos en los que se presume que contienen información digital que es importante para la investigación de un hecho delictivo. (Se deben observar los requisitos de la ley para no violentar derechos y garantías constitucionales, por lo que debe existir orden de juez competente para tal acción). La documentación de la cadena de custodia de la evidencia digital inicia a partir desde los hallazgos de dispositivos de tecnología.

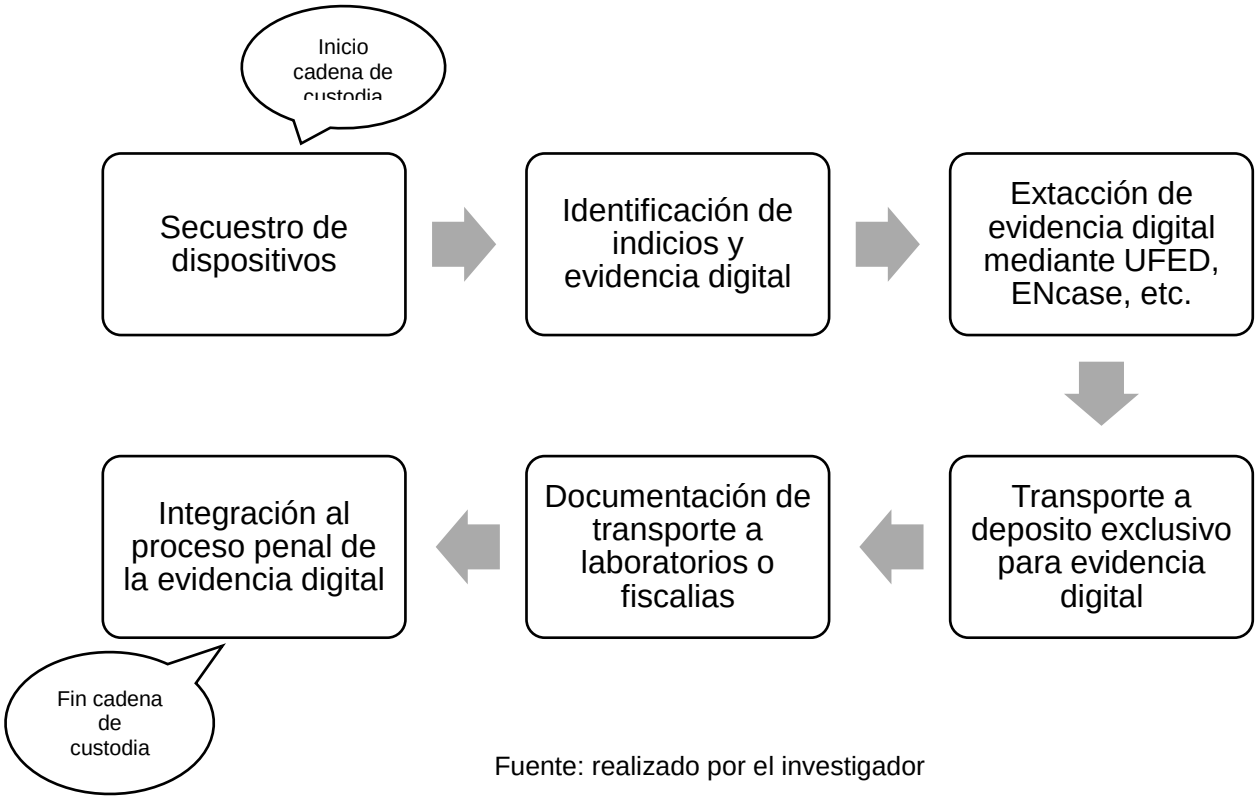
2. La identificación de los indicios o evidencia digital debe versar sobre la relevancia de información o datos según las circunstancias del delito, esto justifica la objetividad del investigador criminal.

3. La extracción de la evidencia digital o información electrónica debe realizarse con dispositivos validados por los entes de investigación e inclusive certificados a nivel internacional, los cuales preserven los archivos en su máxima pureza.

4. Se debe implementar un depósito exclusivo para la evidencia digital, en el cual se pueda documentar y analizar categóricamente cada uno de los indicios o datos digitales, ya que mezclar los dispositivos digitales con otras pruebas puede generar confusión al momento de integrarlo al proceso.

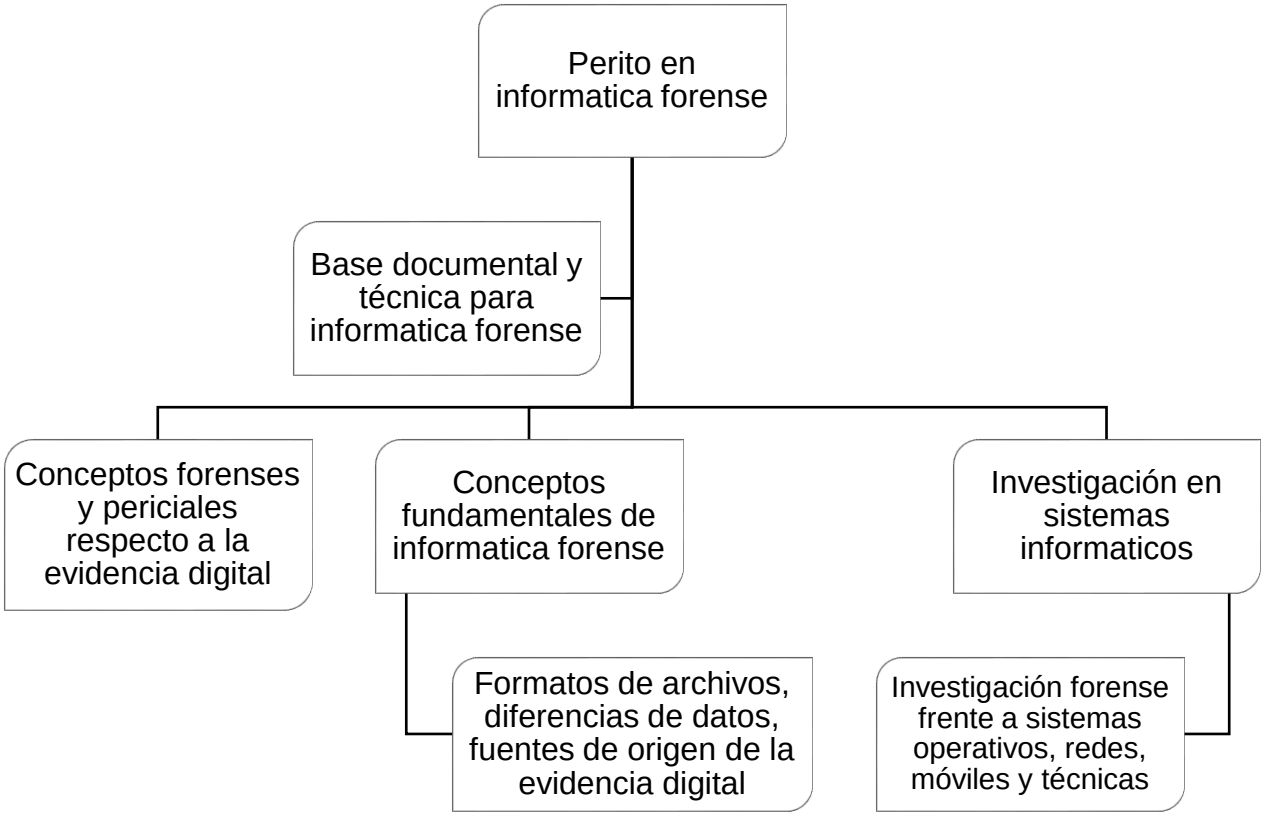
5. Es importante la documentación del traspaso de la evidencia digital a los laboratorios para su análisis o a las diferentes fiscalías para su custodia.

6. La preservación de la evidencia digital y las conclusiones pueden ser sometidas a revisiones de terceros para validar la confiabilidad de los resultados que serán presentados eventualmente en el proceso penal guatemalteco en el cual culmina la cadena de custodia.



Fuente: realizado por el investigador

Asimismo, para se plantea como propuesta novedosa que se consideren los siguientes parámetros para el forense en informática, ya que al comprender la amplia esfera de lo que implica la computación y la informática en la actualidad es necesario que este se mantenga a la vanguardia de las distintas fuentes de evidencia digital, lo que implica capacitaciones constantes y especializaciones en seguridad informática así como en identificación de riesgos que deben tenerse presentes para no afectar a los datos e información sometida a un análisis criminal.



Fuente: realizado por el investigador

En cuanto al objetivo general, ha resultado imposible establecer el manejo de la cadena de custodia y la recolección de la evidencia digital por el Ministerio Público de Guatemala ya que al ser entrevistado el Jefe de la subdirección criminalística operativa DICRI sobre la pregunta ¿Cuál es el procedimiento estandarizado o uniforme para la recolección de evidencia digital en Guatemala, o no existe? Ha

respondido que es un “procedimiento confidencial”,[65] por lo que es importante enfatizar que como institución pública deben brindar información a los interesados media vez no implique que esta sea contraria a la ley, lo que lleva a suponer que este no conoce el procedimiento que existe y si el mismo es a discreción del investigador forense o sigue parámetros uniformes.

En cuanto al objetivo específico consistente: Determinar el debido manejo de la cadena de custodia utilizando distintos software, se ha establecido que en Guatemala se manejan para la efectiva cadena de custodia dispositivos como el UFED, Encase y FTK, los cuales son implementados con exclusividad por algunas fiscalías del departamento del departamento de Guatemala y para cualquier diligencia en los demás departamentos en necesario requerir el auxilio de los mismos; por su parte el objetivo específico orientado a: analizar los mecanismos adecuados para la recolección de evidencia digital, se considera que en Guatemala no existen mecanismos específicos o parámetros definidos con exclusividad a la evidencia digital, al ser entrevistado el Director de la dirección de análisis criminal respecto a la pregunta ¿Cuál es el procedimiento estandarizado o uniforme para la recolección de evidencia digital en Guatemala, o no existe? Ha respondido: “No existe algo específico para la evidencia digital”,[66] y al plantearle la pregunta consistente en: ¿En qué reglamento o ley se encuentra regulado el procedimiento para la cadena de custodia y recolección de la evidencia digital en Guatemala, o no existe? Para lo cual ha respondido “No existe”,[67] estos dos aspectos ponen de manifiesto que en cuanto a la evidencia digital y su respectiva cadena de custodia no existen parámetros procedimentales, lo que lleva a suponer que se implementan las metodologías aplicables a la investigación de evidencia física y tradicional, ignorando por completo los obstáculos y retos que representa la manipulación de datos o información que proviene de dispositivos de tecnología así como la necesidad de estandarizar o uniformizar procedimientos.

[65] Rodríguez, Carlos. *Entrevista trabajo de campo: Manejo de la cadena de custodia en la recolección de evidencia digital*. Guatemala. Jefe de la subdirección criminalística operativa DICRI. 2016.
[66] Director de la dirección de análisis criminal. *Entrevista trabajo de campo: Manejo de la cadena de custodia en la recolección de evidencia digital*. Guatemala. 2016.
[67] *Loc. cit.*

En cuanto al objetivo específico consistente en: definir los procedimientos que realizan los encargados de la recolección de indicios en Guatemala para preservar la evidencia digital, se ha determinado que se desarrolla a través del seguimiento del manual y procedimientos para el procesamiento de la escena de crimen del Ministerio Público como auxiliar para preservar y resguardar los datos e información digital o electrónica recolectada en la escena del crimen. Sin embargo, es importante hacer énfasis en que resulta necesario establecer parámetros, metodologías y procedimientos para cada uno de los distintos sistemas operativos ya que la tecnología a diferencia de la investigación criminal presenta innovaciones a diario y los principales retos yacen en la capacidad del técnico forense en informática en la manipulación de los distintos sistemas operativos, así como los conocimientos avanzados respecto a los distintos formatos que consisten en documentos, archivos, imágenes, videos, audio, imágenes animadas, archivos exclusivos del sistema, registros de acceso, dll's del sistema, virus, troyanos, entre otros. Ya que el verdadero reto proviene de la diferenciación de la información que cada uno de estos eventualmente puede proveer, especialmente en la evolución de los delitos informáticos.

Respecto a la pregunta de investigación formulada de la manera siguiente: ¿Cómo se debe efectuar el debido manejo de la cadena de custodia, desde su inicio para preservar la evidencia digital como propuesta novedosa en los entes encargados de la recolección de evidencia en Guatemala?, es posible responderla a través de las recomendaciones que brinda la Norma ISO 27037 para la Identificación, recolección, adquisición y preservación de la evidencia digital, ya que ante la ausencia de procedimientos uniformes que implemente el Ministerio Público de Guatemala en todas sus sedes regionales y departamentales el auge de la evidencia digital y la necesidad de una adecuada cadena de custodia deben de perfilarse de una forma especializada, técnica y sobre todo objetiva. En este sentido atendiendo a lo que dispone la Norma ISO 27307 respecto a que debe manejarse dentro de la cadena de custodia como requisitos esenciales que van desde minimizar la manipulación de la evidencia digital original, restringiendo el acceso a personas especializadas y

autorizadas que reúnan requisitos categóricos respecto a cada dispositivo, ya que al observar la extensa gama de sistemas operativos, archivos, formatos, registros e información que es posible generarla en la diversidad de dispositivos de tecnología resulta pertinente señalar que cada plataforma presenta su reto por ejemplo Linux, MAC y Windows presentan características muy distintas en su código fuente por lo que examinar información digital que sea potencialmente una evidencia es complejo, por lo que la especialización del perito en informática forense debe ser extensa y abordar la extensa lista de sistemas operativos, para lo cual deben converger una adecuada identificación, recolección, adquisición y preservación de los datos digitales para posteriormente someterse a su respectivo análisis forense criminal.

Por lo que el Ministerio Público y las demás dependencias encargadas de la investigación criminal en Guatemala deben desarrollar procedimientos generales para desarrollar el manejo de la cadena de custodia y las actividades que se relacionan a la recolección de la evidencia digital atendiendo a los principios y requerimientos de relevancia, confiabilidad y suficiencia de la evidencia digital, ya que de esto interdepende muchas veces el resultado del proceso penal; especialmente al debatir sobre la confiabilidad de los datos que se aportan al debate ya que tal como se ha planteado esta evidencia debe ser sometida a un examen de tercero, quien bajo los mismos procedimientos alcanzará el mismos resultado, caso contrario se presentará desconfianza en la evidencia digital y conjuntamente con esta sobre la cadena de custodia registrada. Es por ello, que los requisitos de la cadena de custodia digital deben ser estrictos y especiales atendiendo a la naturaleza así como características de los indicios electrónicos o evidencia digital que es posible generarse en innumerables dispositivos de tecnología.

CONCLUSIONES

1. El debido manejo de la cadena de custodia en la recolección de evidencia digital desde su inicio resulta muy importante en la investigación criminal, esto implica que se desarrollen metodologías locales que observen las propias necesidades y obstáculos que se presentan, como parte de la progresividad en la metodología de la investigación que desarrolla el Ministerio Público de Guatemala.

2. En la actualidad el Ministerio Público y el Centro de recopilación, análisis y difusión de información -Cradic- de Guatemala no cuentan con un procedimiento uniforme para la recolección de la evidencia digital, esto es consecuencia de la falta de una estructura normativa y metodológica que pueda ser puesta a disposición de los profesionales en formación.

3. El manejo de la cadena de custodia utilizando distintos dispositivos de tecnología resulta compleja ya que tal como se ha establecido en el trabajo de campo se utilizan herramientas como FTK, Encase y UFED para los distintos componentes donde se considera que hay evidencias o indicios digitales.

4. La restricción de la información respecto a los procedimientos que utilizan los entes que dirigen la investigación criminal, representa una limitante a los estudios relevantes en cuanto a las nuevos medios de investigación y atendiendo a la transparencia con la que deben actuar es indispensable indicar a cualquier interesado los procedimientos implementados en cuanto a la evidencia digital ya que sin duda alguna implica que se puedan tomar en cuenta los errores en la investigación criminal que puedan influir en la pureza de la evidencia digital y el momento de la integración al proceso penal.

5. El procedimiento estandarizado que propone la Norma ISO 27037 consiste básicamente en la identificación, recolección, adquisición y preservación de la evidencia digital a través de metodologías comprobadas a nivel internacional y

consideradas eficaces para desarrollar la investigación criminal en la esfera de la informática y la computación, esto implica inclusive someter a un estudio de un tercero para alcanzar la confiabilidad de las conclusiones que se deriven del análisis forense sobre datos de tecnología.

6. El estudio de campo practica ha demostrado que no se establecen como requisitos indispensables para el forense informático la especialización en determinadas materias y esto no permite apreciar resultados concretos en cuanto a los estándares mínimos que requieren las instituciones guatemaltecas

RECOMENDACIONES

1. Es recomendable establecer procedimientos uniformes para la recolección de evidencia digital, los cuales observen las normas locales y metodológicas para la investigación criminal en Guatemala especialmente atendiendo a la confiabilidad de todo lo que el perito forense someta a análisis criminal.

2. Se recomienda a las instituciones encargadas de la investigación criminal desarrollar instructivos y manuales que sean útiles para los profesionales en formación, ya que sin duda alguna la como instituciones de carácter público deben proveer la información que sea requerida por cualquier interesado que toda vez la ley no disponga que debe ser confidencial debe encontrarse accesible, esto como parte de la certeza que potencialmente pueden proveer las instituciones a los administrados.

3. Preparar en informática forense a los investigadores de todas las sedes regionales y departamentales del Ministerio Público así como de las instituciones auxiliares de este para que se pueda desarrollar adecuadamente la investigación criminal en la esfera de la informática y la computación.

4. Observar los parámetros internacionales para alcanzar un grado de confiabilidad valido para los tribunales respecto a la cadena de custodia que recae sobre la información y datos digitales que son objeto de investigación criminal.

5. Desarrollar lineamientos basados en cada sistema operativo con la finalidad de delimitar exclusivamente los parámetros de la cadena de custodia digital, procedimientos de identificación, recolección, adquisición y preservación de los indicios y evidencias digitales que sean de interés para la averiguación de la verdad.

REFERENCIAS

Bibliográficas

1. Almeida Romo, Omar Ramiro. Metodología para la implementación de informática forense en sistemas operativos Windows y Linux. Ecuador. Universidad Técnica del Norte. 2011.

2. Arbulora Valverde, Arístides. La cadena de la custodia. Costa Rica. Editorial Marphasa. 2000.

3. Badilla, Jorge. Procesamiento de la escena del crimen. San José, Costa Rica, Escuela Judicial, sección de capacitación organismo de investigación judicial. 1999.

4. Bechimol, Daniel. Hacking desde cero: conozca sus vulnerabilidades y proteja su información. Buenos Aires, Argentina. RerUSERS. 2011.

5. Cano Martínez, Jeimy José. El peritaje informático y la evidencia digital en Colombia: conceptos, retos y propuestas. Colombia. Ediciones Uniandes. 2010.

6. Casado, Laura. Diccionario de Derecho. Argentina. Ediciones Valleta. 2008.

7. Director de la dirección de análisis criminal. Entrevista trabajo de campo: Manejo de la cadena de custodia en la recolección de evidencia digital. Guatemala. 2016.

8. Directores generales de servicios periciales y ciencias forenses. Protocolo de la cadena de custodia. México. Conferencia Nacional de Procuración de Justicia. 2011.

9. Fiscalía General de la Nación. Manual de procedimientos para cadena de custodia. Colombia. 2004.

10. Gervilla Rivas, Carles. Metodología para un análisis forense. España. Universitat Oberta de Catalunya. España. 2014.

11. Guzmán, Carlos. Manual de Criminalística. Buenos Aires, Argentina. Ediciones de la Roca. 2000.

12. Iguarán Arána, Mario German. Manual de procedimientos para cadena de custodia. Colombia. Instituto Nacional de Medicina Legal. 2004.

13. Ministerio de Tecnologías de la Información y Comunicaciones de Colombia. Guía No. 13: sobre seguridad y privacidad de la información que se centra en la evidencia digital. Colombia. MINTIC. 2016.

14. Ministerio Público. Manual de normas y procedimientos para el procesamiento de la escena del crimen. Guatemala. Acuerdo 166-2013.

15. Mora Izquierdo Ricardo y María Dolores Sánchez Prada. La evidencia Física y la Cadena de Custodia dentro del procedimiento penal acusatorio. Bogotá, Colombia. Editores Gráficos. 2007.

16. Ossorio, Manuel. Diccionario de ciencias jurídicas, sociales y políticas. Argentina. Heliasta. 2001.

17. Rodríguez, Carlos. Entrevista trabajo de campo: Manejo de la cadena de custodia en la recolección de evidencia digital. Guatemala. Jefe de la subdirección criminalística operativa DICRI. 2016.

18. Rodríguez, Carlos. Entrevista trabajo de campo: Manejo de la cadena de custodia en la recolección de evidencia digital. Guatemala. Jefe de la subdirección criminalística operativa DICRI. 2016.

19. Romero Guerra, Ana Pamela. La cadena de custodia en el ámbito federal. México. Inacipe. 2010.

Electrónicas

1. Cellebrite delivering mobile expertise. UFED 4PC. Estados Unidos. 2013. Pág. 2. Disponibilidad y acceso: http://www.complexbiz.com/wp-content/uploads/2014/05/UFED-4PC-Brochure_AL_ES_web .pdf fecha de consulta: 02.10.2016.

2. Dabroy, Jahir. La importancia de la labor de inteligencia criminal en Guatemala. Guatemala. RESDAL. 2009. Pág. 5. Disponibilidad y acceso: http://www.resdal.org/jovenes/inteligencia-criminal-dabroy1.pdf. Fecha de consulta: 02.10.2016.

3. García Garduza, Ismael. Diccionario Jurídico. 3ª Edición. México. Editorial Porrúa. 2009. Disponibilidad y acceso: http://www.diccionariojuridico.mx/?pag=vertermi no&id=1704 fecha de consulta 01.03.2016

4. García, José Aurelio. Cadena de custodia vs mismidad. España. Informática Profesional Salmantina. 2016. Disponibilidad y acceso: http://www.informaticoforense.eu/cadena-de-custodia-vs-mismidad/ fecha de consulta. 02.10.2016.

5. Gómez Manrique,Jonathan. Factores que inciden en la alteración de la evidencia digital. Colombia. 2014. Disponibilidad y acceso:

http://informaticaforenseuccaraucacolombia.blogspot.com/2014/05/en sayo-factores-que-inciden-en-la.html fecha de acceso: 29.09.2016.

6. González, Leonardo Emmanuel. 21 herramientas populares de informática forense. 2014. Disponibilidad y acceso: https://prezi.com/kcoki3kq5wsj/21-herramientas-mas-populares-de-informatica-forense/ fecha de consulta: 02.10.2016.

7. Informática Forense Colombia. La evidencia digital. Colombia. 2015. Disponibilidad y acceso: http://www.informaticaforense.com.co/index.php/la-evidencia-digital fecha de consulta: 11.08.2016.

8. López Manrique, Yuri Vladimir. Computación forense: una forma de obtener evidencias para combatir y prevenir delitos informáticos. Guatemala. Universidad San Carlos de Guatemala. 2007. Pág. 31. Disponibilidad y acceso: http://biblioteca.usac.edu.gt/tesis/08/08_0359_CS.pdf fecha de consulta: 11.08.2016.

9. Presman, Gustavo Daniel. ISO/IEC 27037: normalizando la práctica forense informática. Argentina. 1er Congreso Argentino de Ingeniería Forense. 2014. Pág. 8. Disponibilidad y acceso: http://docplayer.es/5605332-Iso-iec-27037-normalizando-la-practica-forense-informatica.html fecha de consulta: 20.11.2016.

10. Ruiz Alquijay, José Daniel. La utilización de la informática forense en los casos de alto impacto social en Guatemala. Guatemala. Universidad San Carlos de Guatemala. 2012. Pág. 57. Disponibilidad y acceso: http://biblioteca.usac.edu.gt/tesis/04/04_10450.pdf fecha de consulta: 11.08.2016.

11. Sánchez Cordero, Pedro. Forensics powertools (listado de herramientas forenses). 2013. Disponibilidad y acceso: http://conexioninversa.blogspot.com/2013/09/forensics-powertools-listado-de.html fecha de consulta: 02.10.2016.

12. Vides Álvarez, Raisa. Evidencia digital. Colombia. Scribd. 2011. Disponibilidad y acceso: https://es.scribd.com/doc/61944356/Evidencia-Digital fecha de consulta: 17.08.2016.

13. Worrall González, Edward C. A. Cadena de custodia. México. Criminalística México. 2014. Dirección de consulta: http://criminalistica.mx/areas-forenses/criminalistica/1568-cadena-de-custodia fecha de consulta: 03.02.16

ANEXOS

Presentación de entrevistas

Universidad Rafael Landívar
Campus de Quetzaltenango
Facultad de Ciencias Jurídicas y Sociales
Tesis: Manejo de la cadena de custodia en la recolección de evidencia digital.
Nombre: Luis Eduardo Escobar de León.

Entrevista

Instrucciones: A continuación se le formularán una serie de interrogantes, mismas que se le solicita amablemente pueda responder. Sus respuestas serán de suma importancia para el desarrollo de la tesis "Manejo de la cadena de custodia en la recolección de evidencia digital", y las mismas serán utilizadas de forma confidencial y con fines estrictamente académicos. Desde ya, se agradece su colaboración al respecto.

Cargo: Jefe de la subdirección criminalística operativa DICRI

Nombre: Ingeniero Carlos Rodríguez

Dependencia: Dirección de Investigación Criminal.

1. **¿Cuál es su concepto respecto a la evidencia digital?**

Es una muestra verificada y certera generada por fuentes informáticas ya sean por medios magnéticos y/o digitales.

2. **¿De qué manera se da la cadena de custodia sobre evidencias e indicios digitales?**

Se da a través de un embalador y/o agente fiscal que garantiza su autenticidad, seguridad, preservación e integridad de la evidencia recolectada.

3. **¿Qué programas o herramientas conoce para la preservación de evidencias digitales?**

UFED, Encase, FTK

4. **¿Cómo se desarrolla la recolección de evidencia digital en la escena del crimen en Guatemala?**

Se desarrolla a través del seguimiento del manual y procedimientos para el procesamiento de la escena de crimen.

5. **¿Qué aspectos son importantes cuidar durante el manejo de evidencia digital en la escena del crimen?**

Su autenticidad, seguridad, preservación e integridad

6. **¿A qué institución se dirigen y en cual se almacenan las evidencias digitales que posteriormente son integradas al proceso penal según su relevancia?**

Ministerio Público

7. **¿Cuál es el procedimiento estandarizado o uniforme para la recolección de evidencia digital en Guatemala, o no existe?**

Es confidencial

8. **¿En qué reglamento o ley se encuentra regulado el procedimiento para la cadena de custodia y recolección de la evidencia digital en Guatemala, o no existe?**

Manual y procedimientos para el procesamiento de la escena de crimen

9. **¿Quién es la persona capacitada para realizar las diligencias de recolección de evidencia digital en la escena del crimen?**

El embalador o Técnico en Escena del Crimen, auxiliares fiscales, agentes fiscales

10. **¿Cuáles son los requisitos que debe reunir el perito para que sea considerado pertinente para diligenciar la evidencia digital?**

Tener certificaciones o capacitaciones que lo avalen

11. **¿Cuáles son los potenciales errores que se comenten en la investigación criminal cuando se trata de indicios o evidencia digital?**

No sé

12. **¿Cuáles son los sistemas operativos que conoce de los que se pueden derivar indicios o evidencia digital (ejemplo: Android, Windows, IOS, etc.)?**
    Android, Windows, IOS.

Muchas gracias por su colaboración

Universidad Rafael Landívar
Campus de Quetzaltenango
Facultad de Ciencias Jurídicas y Sociales
Tesis: Manejo de la cadena de custodia en la recolección de evidencia digital.
Nombre: Luis Eduardo Escobar de León.

Entrevista

Instrucciones: A continuación se le formularán una serie de interrogantes, mismas que se le solicita amablemente pueda responder. Sus respuestas serán de suma importancia para el desarrollo de la tesis "Manejo de la cadena de custodia en la recolección de evidencia digital", y las mismas serán utilizadas de forma confidencial y con fines estrictamente académicos. Desde ya, se agradece su colaboración al respecto.

Cargo: Director de la dirección de análisis criminal DAC

Nombre:

Dependencia: Dirección de Análisis Criminal.

1. **¿Cuál es su concepto respecto a la evidencia digital?**

Es la información recolectada en formato electrónico

2. **¿De qué manera se da la cadena de custodia sobre evidencias e indicios digitales?**

Es la misma cadena utilizada en evidencia documental.

3. **¿Qué programas o herramientas conoce para la preservación de evidencias digitales?**

Ninguno en este departamento

4. **¿Cómo se desarrolla la recolección de evidencia digital en la escena del crimen en Guatemala?**

De la misma forma que la evidencia documental, con el secuestro de dispositivos, computadoras, teléfonos, etc. y toda evidencia electrónica, para posteriormente en departamentos de extracción de información, se recolecte la misma

5. **¿Qué aspectos son importantes cuidar durante el manejo de evidencia digital en la escena del crimen?**

- Individualizar cada dispositivo
- Evitar manipular internamente la información
- Dejar registro en acta acerca de la evidencia recolectada

6. **¿A qué institución se dirigen y en cual se almacenan las evidencias digitales que posteriormente son integradas al proceso penal según su relevancia?**

- Área de informática forense de la dirección de investigación criminalística
- CRADIC

7. **¿Cuál es el procedimiento estandarizado o uniforme para la recolección de evidencia digital en Guatemala, o no existe?**

No existe algo específico para la evidencia digital

8. **¿En qué reglamento o ley se encuentra regulado el procedimiento para la cadena de custodia y recolección de la evidencia digital en Guatemala, o no existe?**

No existe

9. **¿Quién es la persona capacitada para realizar las diligencias de recolección de evidencia digital en la escena del crimen?**

En teoría el área de escena de crimen

10. **¿Cuáles son los requisitos que debe reunir el perito para que sea considerado pertinente para diligenciar la evidencia digital?**

- Conocimiento con pericia informática
- Ideal con capacitaciones en informática forense

11. **¿Cuáles son los potenciales errores que se comenten en la investigación criminal cuando se trata de indicios o evidencia digital?**

Falta de individualización de la evidencia

12. **¿Cuáles son los sistemas operativos que conoce de los que se pueden derivar indicios o evidencia digital (ejemplo: Android, Windows, IOS, etc.)?**

De todos los sistemas operativos se puede generar

Muchas gracias por su colaboración

Entrevista

Instrucciones: A continuación se le formularán una serie de interrogantes, mismas que se le solicita amablemente pueda responder. Sus respuestas serán de suma importancia para el desarrollo de la tesis "Manejo de la cadena de custodia en la recolección de evidencia digital", y las mismas serán utilizadas de forma confidencial y con fines estrictamente académicos. Desde ya, se agradece su colaboración al respecto.

Cargo: Sub dirección general de investigación criminal PNC

Nombre:

Dependencia: Dirección de general de investigación criminal de la Policía Nacional Civil.

1. **¿Cuál es su concepto respecto a la evidencia digital?**

Es todo lo que se encuentra en una escena del crimen de forma electrónica.

2. **¿De qué manera se da la cadena de custodia sobre evidencias e indicios digitales?**

De la misma forma que los demás indicios

3. **¿Qué programas o herramientas conoce para la preservación de evidencias digitales?**

Ninguno en este departamento

4. **¿Cómo se desarrolla la recolección de evidencia digital en la escena del crimen en Guatemala?**

Igual que la de más evidencia

5. **¿Qué aspectos son importantes cuidar durante el manejo de evidencia digital en la escena del crimen?**

Poner por aparte cada dispositivo y dejar constancia de las actas del MP

6. **¿A qué institución se dirigen y en cual se almacenan las evidencias digitales que posteriormente son integradas al proceso penal según su relevancia?**

Al CRADIC o almacén del ministerio público

7. **¿Cuál es el procedimiento estandarizado o uniforme para la recolección de evidencia digital en Guatemala, o no existe?**

Que yo conozca no existe

8. **¿En qué reglamento o ley se encuentra regulado el procedimiento para la cadena de custodia y recolección de la evidencia digital en Guatemala, o no existe?**

Que yo conozca no existe

9. **¿Quién es la persona capacitada para realizar las diligencias de recolección de evidencia digital en la escena del crimen?**

El Ministerio Público

10. **¿Cuáles son los requisitos que debe reunir el perito para que sea considerado pertinente para diligenciar la evidencia digital?**

Debe tener capacitaciones para recolectas las evidencias

11. **¿Cuáles son los potenciales errores que se comenten en la investigación criminal cuando se trata de indicios o evidencia digital?**

Falta de personal capacitado para hacer este trabajo

12. **¿Cuáles son los sistemas operativos que conoce de los que se pueden derivar indicios o evidencia digital (ejemplo: Android, Windows, IOS, etc.)?**

Todos los sistemas operativos se pueden recolectar para la evidencia digital

Muchas gracias por su colaboración