DISEÑO DE UN PROTOCOLO DE VALIDACIÓN Y RECOLECCIÓN DE ELEMENTOS MATERIALES PROBATORIOS Y EVIDENCIA FÍSICA DE TIPO DIGITAL

HEY LENS JAIR PINTO BAUTISTA

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BUCARAMANGA – SANTANDER
2012

DISEÑO DE UN PROTOCOLO DE VALIDACIÓN Y RECOLECCIÓN DE ELEMENTOS MATERIALES PROBATORIOS Y EVIDENCIA FÍSICA DE TIPO DIGITAL

HEY LENS JAIR PINTO BAUTISTA

Director
PhD (c). REINALDO MAYOL ARNAO

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BUCARAMANGA – SANTANDER
2012

DEDICATORIA

Primero a Dios por darme la vida y sabiduría, A mis padres, hermanos, esposa e hijas por ser un impulso en vida para conseguir mis metas.

Hey Lens Jair Pinto Bautista

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

Almacén de evidencias. Lugar donde se almacenan los elementos físicos de prueba, en condiciones ambientales y de seguridad que permitan garantizar la preservación de las mismas.

Almacenamiento. Bodegaje de los elementos materia de prueba y evidencia física en los almacenes de evidencias generales y transitorios teniendo en cuenta las condiciones mínimas necesarias para su conservación.

Análisis. Estudio técnico - científico al lugar de los hechos y a los elementos materia de prueba y evidencia física.

Contaminación. Alterar nocivamente una sustancia u organismo por efecto de residuos procedentes de la actividad humana o por la presencia o manipulación de las mismas.

Criminalística. Es la ciencia auxiliar del derecho (penal, civil, laboral y administrativo, etc) que utiliza o emplea recursos técnico-científicos en la búsqueda y análisis de los elementos materiales de prueba y evidencia física, a fin de establecer si hubo un delito, el autor o autores del mismo y determinar las posibles causas o móviles de lo sucedido, otorgando a los investigadores y al criminalista bases científicas sobre el análisis del lugar de los hechos.

Técnica realizada para el análisis de pruebas. Disciplina que se encarga del descubrimiento y detención de los criminales por métodos científicos. La criminalística como ciencia, estudia las evidencias materiales para investigar un hecho delictivo, en la búsqueda de las pruebas materiales que demuestren la culpabilidad o inocencia de los presuntos responsables. Su contenido se nutre de la medicina legal, de la física, de la química, la fotografía, la balística y la planimetría, etc.

CTI. Cuerpo Técnico de Investigación.

Documento. Escritos, impresos, planos, dibujos, cuadros, fotografías, cintas cinematográficas, discos, grabaciones en medios magnéticos, fonópticas o videos, mensajes de datos, télex, telefax y similares, radiografías, ecografías, tomografías, electroencefalogramas, electrocardiogramas y similares, talones, contraseñas, cupones, etiquetas, sellos y en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares.

Dictamen. Concepto emitido por personas expertas en una ciencia, técnica, arte, oficio o afición, con relación a valoración realizada a un elemento material probatorio y evidencia física y a sus análisis realizados con el lleno de los requisitos legales.

DIJÍN. Dirección de Policía Judicial e Investigación.

Diligencia. Inspección de tipo judicial que se realiza dentro de una investigación. Es el cuidado, actividad y prontitud con que se realiza un acto al que se está jurídicamente obligado. Es toda actuación que realizan el juez, sus auxiliares o comisionados y las partes interesadas dentro de un proceso o con relación a este. Es toda actuación que efectúan los funcionarios públicos en ejercicio de sus respectivas atribuciones y toda actividad que realizan los particulares ante las dependencias del estado u oficiales públicos.

EF. Evidencia Física. Todo elemento tangible que permite objetivar una observación y es útil para apoyar o confrontar una hipótesis.

EMP. Elementos Materiales Probatorios. (I) lo que sea dejado "por la ejecución de la actividad delictiva", (II) los medios utilizados "para la ejecución de la actividad delictiva", (III) los "efectos provenientes de la ejecución de la actividad delictiva",(IV) lo que sea descubierto, recogido y asegurado "en desarrollo de "la diligencia investigativa de registro y allanamiento, inspección corporal y registro personal", (V) "los documentos hallados o que han sido entregados voluntariamente por quien los tenía en su poder o que han sido abandonados",(VI) Lo que se obtiene" "mediante grabación, filmación, fotografía, video o cualquier otro medio avanzado", (VII) Los archivos electrónicos o de intercambio de datos por cualquier medio tecnológico.

Embalaje. Es el procedimiento técnico, utilizado para preservar y proteger en forma adecuada los elementos materia de prueba y evidencia física hallados y recolectados en el lugar de los hechos, lugares relacionados y en las diferentes actuaciones de policía judicial, con el fin de ser enviados a los respectivos laboratorios o bodegas de evidencia.

Escena. Lugar de ocurrencia de un acto delictivo. Entiéndase en la investigación criminal como cualquier lugar mueble o inmueble donde se presuma la comisión de un hecho punible y el sitio en donde se sospeche la presencia de elementos materia de prueba y evidencia física relacionada con la misma.

Estandarizar. Unificar procedimientos.

Fijar. Volver inalterable una imagen. Forma de perpetuar con exactitud el lugar de los hechos y los EMP Y EF relacionados con este.

Indagación. Etapa pre procesal en la que la Fiscalía General de la Nación, a través de la Policía Judicial, adelanta labores investigativas y recauda EMP, EF o información pertinente, con el objeto de determinar la existencia de una conducta delictiva e individualizar a los autores o partícipes.

Informe. Entiéndase como el documento que rinden los funcionarios de policía Judicial o quienes hagan sus veces por vía de excepción, en el cual se plasman todas las actividades desplegadas durante la indagación e investigación con los requisitos de ley.

Investigación. Fase de la investigación en la que la Fiscalía General de la Nación, con apoyo de la Policía Judicial, busca complementar y adicionar EMP, EF o información pertinente que fortalezca la teoría del caso.

Juicio. Decisión o sentencia de un tribunal.

Medio de prueba. Instrumentos o elementos de que se vale el juez y las partes para aportar la verdad al proceso. Así: la confesión, el testimonio de terceros, el dictamen pericial, los documentos, la inspección judicial, los indicios. En el proceso civil, el juramento, como medio especial de prueba.

Prueba pericial. Medio de prueba legal que consiste en los análisis científicos que realizan los expertos en las diferentes ciencias, disciplinas y artes que aplican a la investigación criminal.

SIJÍN. Seccional de Policía Judicial e Investigación

RESUMEN

En este documento se presenta la propuesta de la elaboración de un protocolo de validación para el manejo y recolección de elementos materiales probatorios y evidencia física de tipo digital que se puedan hallar en una escena donde posiblemente se halla cometido un delito. Documento que permitirá tener un adecuada información que ayudara a evitar cualquier alteración, contaminación y pérdida de datos y/o información contenidos en dispositivos digitales ya sea en al momento de su identificación, recolección y embalaje.

Así mismo se destaca la manera como se deben manipular dichos elementos contando con una secuencia objetiva, clara y precisa para su recolección una vez sean hallados. De igual manera tener claro que elementos son los apropiados para embalarlos ya que permitirán tener cuidado acerca de su manipulación y con esto contribuir a la conservación de los mismos, teniendo en cuenta la fragilidad que estos tienen.

El protocolo de recolección proporciona aspectos importantes que ayuda a tener un adecuado manejo de las evidencias, garantizando que los elementos no han sido alterados o modificados por cualquier factor ya sea ambiental, eléctrico, entre otros y con esto evitar su exclusión en un estrado judicial por lo que permitirá demostrar la responsabilidad de un hecho investigado.

ABSTRACT

This document presents the proposal for the development of a validation protocol for the management and collection of material evidence and physical evidence of digital type that can be found in a scene where is possibly a crime. Document that will have adequate information to help avoid any alteration, pollution and loss of data and / or information contained in digital devices either at the time of identification, collection and packaging.

It also highlights how these elements should be handled with a sequence counting objective, clear and precise for collection once they are found. Likewise, be aware that items are appropriate to package and that will take care about handling and thereby contribute to their conservation, taking into account the fragility that they have.

The collection protocol provides important aspects helps to have a proper handling of evidence, ensuring that the elements have not been altered or modified by any factor either environmental, electrical, etc. and thereby prevent its removal on a judicial bench which will demonstrate the responsibility of the offense under investigation

INTRODUCCION

Los Elementos Materiales Probatorios y Evidencias Físicas (EMP y EF en lo sucesivo) son en realidad los argumentos de convicción que tienen las partes intervinientes en una investigación forense. Por tal razón, es imprescindible tener métodos, procedimientos y herramientas que faciliten, con muy poco margen de error, la adquisición, validación y procesamiento de evidencias. Un caso especialmente importante de este tipo de procedimiento ocurre cuando se procesa evidencia que puede convertirse en procesos penales. Es necesario, en estos casos, plantear una metodología basada en un protocolo técnico – científico para el procesamiento de una escena donde se haya cometido un delito.

Es importante tener en cuenta que los EMP y EF de tipo digital hallados en una escena tiene una gran fragilidad debido, entre otros factores, a su volatilidad. Desafortunadamente, la falta de procedimientos formalmente establecidos y respetados produce la pérdida irreparable de información importante tales como contenidos de memoria, estado de procesos y otros. Otro elemento importante es el manejo adecuado de las cadenas de custodia ya que se garantiza la autenticidad de los datos e intervinientes que tengan contacto con las evidencias.

Este documento describe una propuesta para la realización protocolo de validación y recolección de elementos materiales probatorios y evidencia física de tipo digital para el Cuerpo Técnico de Investigación de la Fiscalía General de la Nación.

1. PROBLEMA

1.1 DEFINICION DEL PROBLEMA

El Cuerpo Técnico de Investigación (C.T.I) es una entidad de carácter oficial perteneciente a una de las áreas de la Fiscalía General de la Nación. La institución cuenta con diversos laboratorios tales como Química, Genética, Balística, Documentologia, Lofoscopia, Informática y Forense que requieren un protocolo estricto de recolección de evidencias. En la actualidad sólo se cuenta con un instructivo para procedimientos de recolección pero este tiene muchos vacíos con respecto a los diferentes elementos digitales que se puedan hallar en una escena. Esta carencia de elementos formales y completos limita y compromete la efectividad real de los procesos de peritaje, análisis y presentación de elementos probatorios desde el punto de vista operativo como legal.

Por lo tanto, contar con un protocolo de recolección de EMP y EF formulado y probado, donde se establezcan los procedimientos y las actividades para lograr un adecuado, correcto y completo procesamiento de las escenas y que permita obtener elementos que sean conducentes para la investigación, contribuirá a la administración de justicia de manera real y efectiva.

1.2 JUSTIFICACION

Recientemente se ha registrado un aumento en los delitos donde intervienen elementos digitales [1] incluyendo múltiples medios de almacenamiento donde se puedan obtener elementos para determinar responsabilidad directa en la comisión de un delito. En Colombia existe una normatividad [2] ley 1273 de 2009 que protege el bien jurídicamente tutelado por el estado, (datos e información, según la terminología del propio instrumento jurídico). Por lo tanto, se debe tener en cuenta este concepto en los lugares donde se puedan descubrir, recolectar y embalar EMP y EF.

La masificación de acceso de usuarios a Internet ha contribuido a la creación de nuevas modalidades de hurto y prácticas delincuenciales con este tipo de herramientas de tecnología y telecomunicaciones. [1]

Se han podido identificar diferentes tipos de delitos. [1], entre los que se encuentran aquellos que:

- **Afectan el patrimonio económico:** falsificación de datos en banca virtual, phishing, keyloggers, compra y venta a través de falsos portales, falsos premios.

- **Buscan el abuso de menores:** comercialización de videos, fotografía, audio, texto, falsas agencias, bulling y otros.

- **Afectan la propiedad intelectual:** descargas de programas y comercialización de obras sin pagar derechos de autor.

- **Afectan la información como bien jurídico:** empleados que usan sus privilegios o permisos para acceder a información que es secreto de la empresa y luego entregarla a la competencia.

Según estadísticas del Grupo de Investigación de Delitos Informáticos de la Dirección Central de Policía Judicial (DIJIN), el cual se dedica a la investigación de conductas delictivas derivadas del uso de la tecnología y telecomunicaciones, el hurto a través de Internet es uno de los mayores delitos que se presentan en Colombia**.** [1]

En el año 2010 los delitos a través de internet se dispararon en el país, la situación es tan delicada que diariamente el CAI virtual de la Policía Nacional está recibiendo en promedio 1.700 quejas o denuncias por uso indebido de herramientas como Facebook y otras redes sociales. Las autoridades precisaron que las amenazas, instigación al delito, injurias, calumnias y suplantación son los delitos que más se están cometiendo a través de internet. [3]

Según aporte realizado por las Unidades de Delitos Informáticos del CTI y la DIJIN los casos llevados durante el año 2009 y 2010 aproximadamente el 80% el delito que mayor impacto tuvo fue el Hurto por medios informáticos y semejantes. [4]. En los procesos de indagación, investigación y acusación etapas del sistema penal acusatorio colombiano soportado por el ente acusador que es la Fiscalía General de la Nación, quien tiene la responsabilidad de la carga probatoria, la prioridad es la preservación de los elementos materiales probatorios y evidencias físicas hallados y recolectados en los lugares donde se cometió un delito. Razón por la cual se hace necesario otorgar la debida importancia en el manejo de estos elementos, más aún cuando son de tipo digital.

Por los motivos expuestos se tiene la necesidad de la realización de un protocolo para el procesamiento de una escena, donde se hallen elementos EMP y EF de tipo digital por el Cuerpo Técnico de Investigación de la Fiscalía General de la Nación. Este procedimiento debe redundar en la calidad de los elementos del sistema de cadena de custodia que permitirán obtener los niveles adecuados de

seguridad, integridad, eficiencia y efectividad para asegurar las características originales de los elementos desde su recolección hasta su disposición final con la presentación en el juicio y su posterior admisión como prueba.

1.3 OBJETIVOS

1.3.1 Objetivo General.

Diseñar un protocolo de recolección y validación de elementos materiales probatorios y evidencia física de tipo digital hallados en el procesamiento de una escena por el cuerpo técnico de investigación de la fiscalía general de la nación.

1.3.2 Objetivos Específicos.

- Determinar qué tipo de elementos físicos y digitales se definen como elementos materiales probatorios y evidencia física en una escena.

- Establecer un método para evitar la contaminación o pérdida de los elementos digitales hallados en una escena.

- Diseñar y normalizar los procedimientos para la recolección, embalaje y el tratamiento de elementos materiales probatorios y evidencia física de tipo digital.

- Definir elementos apropiados para el embalaje y almacenamiento de los elementos materiales probatorios y evidencia física de tipo digital.

1.4 DELIMITACIONES

1.4.1 Temporal

El desarrollo del proyecto se desarrollara en un tiempo de 6 meses a partir del momento de aprobación del anteproyecto.

1.4.2 Contextual

1.4.2.1 Políticas Institucionales del Cuerpo Técnico de Investigación

1.4.2.1.1 Visión: Ser reconocidos como una entidad del Estado eficaz en la investigación penal, encontrando la verdad de la conducta punible, con sujeción a la ley y respeto al debido proceso, en procura del restablecimiento del derecho y de la justicia restaurativa, afianzando la credibilidad de la ciudadanía en la administración de la justicia. [5]

1.4.2.1.2 Misión: Garantizar el acceso a una justicia eficaz y oportuna con el fin de encontrar la verdad dentro del marco del respeto por el debido proceso y las garantías constitucionales. [5]

1.4.2.1.3 Ubicación Geográfica: El Cuerpo Técnico de Investigación – C.T.I es una entidad de orden nacional siendo esta la policía judicial de la Fiscalía General de la Nación, pertenecientes a la rama judicial con autonomía administrativa y presupuestal. Conformada por el Fiscal General de la Nación quien es la máxima autoridad de la entidad, quien a su vez delega las actuaciones a cada una de la Direcciones Nacionales de Fiscalía y Cuerpo Técnico de Investigación y así mismo a las direcciones seccionales llevando la aplicación de justicia a las unidades de policía judiciales conformadas por jurisdicciones y aplicación en todo el país.

El nivel central de la Fiscalía General de la Nación se encuentra ubicado en la ciudad de Bogotá D.C. conocido como el “Bunker” situado en la Diagonal 22B No. 52-01 (Ciudad Salitre).

1.4.2.2. Historia de la Fiscalía General de la Nación. La Fiscalía General nació en 1991, con la promulgación de la nueva Constitución Política y empezó a operar el 1 de julio de 1992.

Es una entidad de la rama judicial del poder público con plena autonomía administrativa y presupuestal, cuya función está orientada a brindar a los ciudadanos una cumplida y eficaz administración de justicia. [5]

1.4.2.3. Principios fundamentales del Cuerpo Técnico de Investigación.

1.4.2.3.1. Funciones: La Fiscalía General se encarga de investigar los delitos, calificar los procesos y acusar ante los jueces y tribunales competentes a los presuntos infractores de la ley penal, ya sea de oficio o por denuncia.

La investigación de oficio se realiza por iniciativa propia del Estado y la investigación por denuncia cuando existe un tercero es víctima de un delito e instaura la denuncia ante alguna de las autoridades competentes (Comisaría, Inspección de Policía o Unidad de Reacción Inmediata de la Fiscalía, URI).

1.4.2.3.2. Limitaciones: La Fiscalía General no juzga a los presuntos autores o partícipes de un delito. Esta función corresponde, previa acusación de la Fiscalía, a los jueces y tribunales de la República. Estos, de acuerdo con las pruebas practicadas en la investigación y el juzgamiento, condenan o absuelven a los acusados. En el primer caso indican la pena a que debe someterse el sentenciado.

La Fiscalía General no investiga los delitos cometidos por militares en razón de sus funciones, ni los delitos cometidos por congresistas cuya investigación y juzgamiento corresponde a la Corte Suprema de Justicia, ni los delitos cometidos por menores de edad, ni las contravenciones, ni resuelve conflictos administrativos, laborales, familiares o civiles.

1.4.2.4. Pilares del Cuerpo Técnico de Investigación

1.4.2.4.1. Indagación Penal. Una vez se produce un hecho jurídicamente relevante que puede constituir delito querellable o perseguible de oficio, la policía judicial (Policía Nacional SIJIN, DIJIN, Cuerpo Técnico de Investigación – C.T.I, Departamento Administrativo de Seguridad -DAS- o Policía de Tránsito, o aquellas dependencias que transitoriamente pueden cumplir esa función- asumen la indagación para la práctica de las primeras diligencias o aquellas urgentes para descubrir y asegurar los elementos materiales probatorios, las evidencias físicas o los informes legalmente ofrecidos, actuando como primeros respondientes.

Se notará entonces un protagonismo de la policía judicial, un gran compromiso investigativo y enorme responsabilidad de todas las actividades y pesquisas que pueden desarrollar los investigadores, porque después en las audiencias públicas preliminares o de fondo pueden ser llamados y deben comparecer como testigos para que delante de la comunidad enfrenten a la delincuencia y constituyan el centro probatorio en procura de la verdad.

No existe un término establecido legalmente para realizar las labores de indagación, particularmente cuando no se ha sorprendido in flagranti delictu o capturado en flagrancia al autor o partícipe de la conducta penal. Pero han de tenerse en cuenta los términos o plazos legales de la prescripción de la acción penal o los términos para presentar la querella en los delitos que no son perseguibles oficiosamente. [6]

1.4.3 Espacial

El desarrollo y la implementación del proyecto se harán para el cuerpo Técnico de Investigación – C.T.I. de la Fiscalía General de la Nación con un alcance nacional esperado.

2. MARCO REFERENCIAL

2.1. MARCO HISTÓRICO

2.1.1 Antecedentes Investigativos

En el trabajo realizado por Giovanni Zuccardi - Juan David Gutiérrez, denominado Infraestructura para la gestión de la evidencia digital en redes inalámbricas, muestra desde una perspectiva los aspectos de seguridad que se debe tener en las redes inalámbricas es un aspecto crítico que no se puede descuidar. Debido a que las transmisiones viajan por un medio abierto (el aire, al cual tiene acceso cualquiera), se requieren mecanismos que aseguren la confidencialidad de los datos así como su integridad y autenticidad. En estos términos visualiza los aspectos relevantes al cuidado que se debe tener y de darse algún hecho que amerite investigación, los protocolos utilizados dejaran trazabilidad que orientaran de manera clara a la obtención de elementos de prueba. [7]

Así mismo muestra Zuccardi y Gutiérrez en el trabajo denominado Informática forense, en donde exponen la aplicación de procedimientos estrictos y rigurosos puede ayudar a resolver grandes crímenes apoyándose en el método científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales. [8]

Por otro lado el Dr. Vladimir Covarrubias L, en su investigación denominado Protocolo Informático Forenses 7 Fases, describe unos proceso de recopilación de evidencias de eventos posee 3 componentes esenciales; **Técnico** que contribuye en la búsqueda de indicios y bitácoras de auditoría, **Pericial** en que el Perito examina y transforma la evidencia en medios de prueba y finalmente fase **Legal y de comunicación**, en que el asesor legal denunciará el delito apoyado en el informe pericial. [9]

2.2. MARCO TEORICO – CONCEPTUAL

Casey define la evidencia de digital como “cualquier dato que puede establecer que un crimen se ha ejecutado (commit) o puede proporcionar una enlace (link) entre un crimen y su víctima o un crimen y su autor”. [10]

De acuerdo con la publicación HB:171 2003 *Guidelines for the Management of IT Evidence,* [11] 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”. Esta puede ser dividida en tres categorías.

1.- Registros almacenados en el equipo de tecnología informática (p.e., correos electrónicos, archivos de aplicaciones de ofimática, imágenes, etc).

2.- Registros generados por los equipos de tecnología informática (registros de auditoría, registros de transacciones, registros de eventos, etc).

3.- Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática (hojas de cálculo financieras, consultas especializadas en bases de datos, vistas parciales de datos, etc).

La evidencia digital es la materia prima para los investigadores donde la tecnología informática es parte fundamental del proceso. Sin embargo y considerando el ambiente tan cambiante y dinámico de las infraestructuras de computación y comunicaciones, es preciso detallar las características propias de dicha evidencia en este entorno.

La evidencia digital, para aquellos que la identifican y analizan en la búsqueda de la verdad, posee, entre otros elementos que la hacen un constante desafío, las siguientes características: [11]

1.- Es volátil
2.- Es anónima
3.- Es duplicable
4.- Es alterable y modificable
5.- Es eliminable

Estas características nos advierten sobre la exigente labor que se requiere por parte de los especialistas en temas de informática forense, tanto en procedimientos como en técnicas y herramientas tecnológicas para obtener, custodiar, revisar, analizar y presentar la evidencia presente en una escena del delito. Por tanto, es necesario mantener un conocimiento detallado de las normas y regulaciones legales asociadas con las pruebas y el derecho procesal, así como de las técnicas y los procesos que permitan mantener la confiabilidad de los datos recogidos, la integridad de los medios, el análisis detallado de los datos y la presentación idónea de los resultados. [11]

Los Elementos Materiales Probatorios y Evidencia Física – “EMP y EF” recolectados en un lugar donde se haya cometido un delito ya sea tradicional o a través de medios digitales o electrónicos y en las condiciones en que se haya

realizado es necesario que sea sometido a un sistema que lo proteja y salvaguarde con el fin de que no sean alterados en su integridad.

Una vez hallados, recolectados y embalados técnicamente, se someten a un sistema documentado que se aplica a los EMP y EF por las personas responsables del manejo de los mismos, desde el momento en que se encuentran o aportan a la investigación hasta su disposición final, lo que permite no solo garantizar su autenticidad, sino demostrar que se han aplicado procedimientos estandarizados para asegurar las condiciones de identidad, integridad, preservación, seguridad, continuidad y registro.

Este sistema se aplica a los EMP y EF recolectados en el lugar de los hechos u otros lugares. Para demostrar su autenticidad se basa en los siguientes principios:

- Identidad: Es la individualización de los EMP y EF mediante la descripción completa y detallada de todas sus características, teniendo en cuenta los pasos de descripción objetiva de cada elemento o sustancia como: color, peso, forma, cantidad, medida, volumen, tipo de construcción y estado, entre otros.[12]

- Integridad: Determina que el EMP y EF allegado a la investigación conforme al debido proceso es el mismo que se está utilizando para tomar una decisión judicial. [12]

- Preservación: Es asegurar las condiciones adecuadas de conservación e inalterabilidad de los EMP y EF de acuerdo con su clase y naturaleza. [12]

- Seguridad: Está a cargo de los custodios, quienes deberán mantener libres y exentos de todo riesgo y peligro a los EMP y EF. [12]

- Almacenamiento: Es la acción o efecto de guardar los EMP y EF bajo condiciones adecuadas para garantizar su preservación y protección. [12]

- Continuidad y Registro: Es la secuencia ininterrumpida de todos los traslados y traspasos de los EMP y EF entre custodios, garantizada mediante el registro único de cadena de custodia. [12]

- La cadena de custodia se inicia en el lugar donde se descubren, encuentren o recauden los EMP y EF. De esta manera la aplicación de la cadena de custodia es responsabilidad de los servidores públicos y particulares que por razón de su trabajo o por el cumplimiento de las funciones entren en contacto con los EMP y EF. Esta consiste en la recolección, preservación y entrega de los mismos a la autoridad correspondiente. [13]

La importancia de utilizar los procesos y las herramientas forenses informáticas garantizan que la identificación, obtención y análisis forense no alterará la evidencia, permitiendo poder avanzar en la identificación del crimen informático y ubicar responsables, dando inicio a la formalización legal de los hechos a través de denuncia o querella en lo Penal, Civil o Laboral, con la certeza que la evidencia permanece inalterable y con el apoyo de un informe forense informático que avala en una exposición y análisis técnico los dichos legales conforme a derecho. [9]

2.3 MARCO LEGAL

2.3.1 Ley 1273 de Enero 5 de 2009

"Por medio de la cual se modifica el Código Penal Colombiano, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". [14]

2.3.2 Ley 599 del 24 de Julio de 2000. Artículo 257. De la prestación, acceso o uso ilegales de los servicios de telecomunicaciones

<Artículo modificado por el artículo 1 de la Ley 1032 de 2006. El nuevo texto es el siguiente:> El que, sin la correspondiente autorización de la autoridad competente, preste, acceda o use servicio de telefonía móvil, con ánimo de lucro, mediante copia o reproducción de señales de identificación de equipos terminales de estos servicios, o sus derivaciones, incurrirá en prisión de cuatro (4) a diez (10) años y en multa de quinientos (500) a mil (1.000) salarios mínimos legales mensuales vigentes.

En las mismas penas incurrirá el que, sin la correspondiente autorización, preste, comercialice, acceda o use el servicio de telefonía pública básica local, local extendida, o de larga distancia, con ánimo de lucro.

Iguales penas se impondrán a quien, sin la correspondiente autorización, acceda, preste, comercialice, acceda o use red, o cualquiera de los servicios de telecomunicaciones definidos en las normas vigentes.

PARÁGRAFO 1o. No incurrirán en las conductas tipificadas en el presente artículo quienes en virtud de un contrato con un operador autorizado comercialicen servicios de telecomunicaciones.

PARÁGRAFO 2o. Las conductas señaladas en el presente artículo, serán investigables de oficio.

2.3.3 Ley 1266 del 31 de diciembre de 2008

Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. [15]

2.3.4 Ley 906 del 31 de Agosto de 2004

Por la cual se expide el Código de Procedimiento Penal Colombiano [16]

2.3.4.1 Artículo 213. Inspección del lugar del hecho. Inmediatamente se tenga conocimiento de la comisión de un hecho que pueda constituir un delito, y en los casos en que ello sea procedente, el servidor de Policía Judicial se trasladará al lugar de los hechos y lo examinará minuciosa, completa y metódicamente, con el fin de descubrir, identificar, recoger y embalar, de acuerdo con los procedimientos técnicos establecidos en los manuales de criminalística, todos los elementos materiales probatorios y evidencia física que tiendan a demostrar la realidad del hecho y a señalar al autor y partícipes del mismo.

El lugar de la inspección y cada elemento material probatorio y evidencia física descubiertos, antes de ser recogido, se fijarán mediante fotografía, video o cualquier otro medio técnico y se levantará el respectivo plano.

La Fiscalía dispondrá de protocolos, previamente elaborados, que serán de riguroso cumplimiento, en el desarrollo de la actividad investigativa regulada en esta sección. De toda la diligencia se levantará un acta que debe suscribir el funcionario y las personas que la atendieron, colaboraron o permitieron la realización.

2.3.4.2 Artículo 236. Recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes. Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o el imputado ha estado transmitiendo información útil para la investigación que se adelanta, durante su navegación por internet u otros medios tecnológicos que produzcan efectos equivalentes, ordenará la aprehensión del computador, computadores y servidores que pueda haber utilizado, disquetes y demás medios

de almacenamiento físico, para que expertos en informática forense descubran, recojan, analicen y custodien la información que recuperen.

En estos casos serán aplicables analógicamente, según la naturaleza de este acto, los criterios establecidos para los registros y allanamientos.

La aprehensión de que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida. Inmediatamente se devolverán los equipos incautados.

2.3.4.3 Capitulo V - Cadena de custodia. - Artículo 254. Aplicación. Con el fin de demostrar la autenticidad de los elementos materiales probatorios y evidencia física, la cadena de custodia se aplicará teniendo en cuenta los siguientes factores: identidad, estado original, condiciones de recolección, preservación, embalaje y envío; lugares y fechas de permanencia y los cambios que cada custodio haya realizado. Igualmente se registrará el nombre y la identificación de todas las personas que hayan estado en contacto con esos elementos.
La cadena de custodia se iniciará en el lugar donde se descubran, recauden o encuentren los elementos materiales probatorios y evidencia física, y finaliza por orden de autoridad competente.

PARÁGRAFO. El Fiscal General de la Nación reglamentará lo relacionado con el diseño, aplicación y control del sistema de cadena de custodia, de acuerdo con los avances científicos, técnicos y artísticos.

2.3.4.4 Artículo 257. Inicio de la cadena de custodia. El servidor público que, en actuación de indagación o investigación policial, hubiere embalado y rotulado el elemento material probatorio y evidencia física, lo custodiará.

2.3.4.5 Capitulo único. - Elementos materiales probatorios, evidencia física e información - Artículo 275. Elementos materiales probatorios y evidencia física. Para efectos de este código se entiende por elementos materiales probatorios y evidencia física, los siguientes:

a) Huellas, rastros, manchas, residuos, vestigios y similares, dejados por la ejecución de la actividad delictiva.

b) Armas, instrumentos, objetos y cualquier otro medio utilizado para la ejecución de la actividad delictiva.

c) Dinero, bienes y otros efectos provenientes de la ejecución de la actividad delictiva.

d) Los elementos materiales descubiertos, recogidos y asegurados en desarrollo de diligencia investigativa de registro y allanamiento, inspección corporal y registro personal.

e) Los documentos de toda índole hallados en diligencia investigativa de inspección o que han sido entregados voluntariamente por quien los tenía en su poder o que han sido abandonados allí.

f) Los elementos materiales obtenidos mediante grabación, filmación, fotografía, video o cualquier otro medio avanzado, utilizados como cámaras de vigilancia, en recinto cerrado o en espacio público.

g) El mensaje de datos, como el intercambio electrónico de datos, internet, correo electrónico, telegrama, télex, telefax o similar, regulados por la Ley 527 de 1999 o las normas que la sustituyan, adicionen o reformen.

h) Los demás elementos materiales similares a los anteriores y que son descubiertos, recogidos y custodiados por el Fiscal General o por el fiscal directamente o por conducto de servidores de policía judicial o de peritos del Instituto Nacional de Medicina Legal y Ciencias Forenses, o de laboratorios aceptados oficialmente.

2.3.4.6 Artículo 276. Legalidad. La legalidad del elemento material probatorio y evidencia física depende de que en la diligencia en la cual se recoge o se obtiene, se haya observado lo prescrito en la Constitución Política, en los Tratados Internacionales sobre derechos humanos vigentes en Colombia y en las leyes.

2.3.4.7 Artículo 277. Autenticidad. Los elementos materiales probatorios y la evidencia física son auténticos cuando han sido detectados, fijados, recogidos y embalados técnicamente, y sometidos a las reglas de cadena de custodia.

La demostración de la autenticidad de los elementos materiales probatorios y evidencia física no sometidos a cadena de custodia, estará a cargo de la parte que los presente.

2.3.5 Resolución 0-2869 de diciembre 29 de 2003, de la Fiscalía General de la Nación

Por medio de la cual se adoptó el manual de procedimientos de cadena de custodia. [17]

2.3.6 Resolución 0-6394 de diciembre 22 de 2004, de la Fiscalía General de la Nación

Por medio de la cual se adopta el manual de procedimientos de cadena de custodia para el sistema penal acusatorio. [18]

3. DISEÑO METODOLOGICO

3.1. TIPO DE INVESTIGACIÓN

La investigación propuesta es de tipo empírico, primaria. Como primer paso se definirán un grupo de requisitos necesarios para la correctitud de los procesos de recolección de evidencia. El marco referencial de este proceso está dado por las buenas prácticas comúnmente aceptadas y los requisitos que exigen los procesos legales colombianos.

Como segundo paso se definirán en un nivel más bajo de abstracción cuales son los elementos que normalmente se requieren por tipos de dispositivos y evidencias.

Se trabajará con un modelo estructural de matrices definiendo los requisitos formales y metodológicos de cada proceso sobre cada tipo de evidencia o dispositivos.

Finalmente se realizará un proceso de pruebas sobre datos reales y datos sintéticos.

4. ESQUEMA TEMATICO

4.1. TIPO DE ELEMENTOS FÍSICOS Y DIGITALES QUE SON ELEMENTOS MATERIALES PROBATORIOS Y EVIDENCIA FÍSICA EN UNA ESCENA.

En una escena donde se haya cometido un delito existe la posibilidad de que quien lo haya realizado deje rastros o elementos que permitan inferir lógicamente a las personas que la procesan establecer hipótesis válidas de lo sucedido una vez hayan sido recolectadas. [19]

Se puede decir que el término “Evidencia Digital” abarca cualquier información en formato digital que pueda establecer una relación entre un delito y su autor [19]. Desde el punto de vista del derecho probatorio, puede ser comparable con “un documento” como prueba legal.

La evidencia digital debe cumplir con algunos requerimientos para tener validez jurídica [19].

- ✓ Autenticidad: La evidencia no ha sido modificada
- ✓ Precisión: Tanto las herramientas, como los procedimientos no deben presentar dudas, además debe estar relacionada con el incidente
- ✓ Suficiencia: Debe mostrar todo los eventos que relacionan a un incidente

De acuerdo a la naturaleza del delito, así también es la pertinencia objetiva de los elementos que se puedan hallar en una escena, por tanto los elementos físicos con información digital almacenada los podemos realizar una clasificación de acuerdo a su funcionalidad así:

EQUIPOS DE CÓMPUTO

- Computador Portátil
- Computador De Escritorio
- Computador Tipo Servidor
- Tablet PC

DISPOSITIVOS DE COMUNICACIÓN DE DATOS

- Router
- Firewall
- VPN

DISPOSITIVOS DE CAPTURA DE DATOS, AUDIOS E IMÁGENES

- DVR
- Grabadoras Digitales
- Reproductores MP3, MP4, MP5
- Cámaras Fotográficas
- Cámaras de Video

EQUIPOS DE COMUNICACIÓN

- Teléfonos Celulares
- IPod – IPad
- IPhone
- Palm – Pocket – PDA

SISTEMAS DE ALMACENAMIENTO

A gran escala

- Sistemas de Discos Raid – Arreglo de Discos
- Sistemas SAN – Clúster

Portable

De tipo óptico

- CD - DVD
- Duplicadora de Discos

De tipo magnético

- Diskettes
- Discos Duros (IDE – ATA – SATA - SCSI)
- Discos Duros Externos
- Micro Drive
- Cintas Magnéticas
- Discos ZIP

De tipo removible

- Memorias USB
- Memorias (SD – Micro SD – MMC – XD)
- Sim Card de Teléfonos Móviles Celulares

SISTEMAS DE IMPRESIÓN

- Copiadoras – Fotocopiadoras
- Impresoras
- Fax

OTROS DISPOSITIVOS

- GPS
- Juegos Electrónicos – X box

Esta clasificación se da a raíz de las diferentes formas como es almacenada en los diferentes dispositivos, teniendo en cuenta su funcionalidad y uso. Por lo que es la manera más adecuada para establecer dicha clasificación. Una vez conocido los diferentes medios donde se puede hallar datos y/o información en medios de almacenamiento digitales en una escena, se puede concluir que "…La evidencia digital es la materia prima para los investigadores donde la tecnología informática es parte fundamental del proceso. Sin embargo y considerando, el ambiente tan cambiante y dinámico de las infraestructuras de computación y comunicaciones, es preciso detallar las características propias de dicha evidencia en este entorno…"

4.2. MÉTODO PARA EVITAR LA CONTAMINACIÓN O PÉRDIDA DE LOS ELEMENTOS DIGITALES HALLADOS EN UNA ESCENA.

Una vez en la escena donde posiblemente se ha cometido un delito o se ha vulnerado un derecho, es importante tener en cuenta que los elementos de tipo digital hallados son frágiles y volátiles por lo que se debe tener mucho cuidado en evitar contaminarlos para que al momento de ser presentado ante un juez estos sean admitidos, de esta manera hay que conservar y garantizar su integridad, identidad, autenticidad, continuidad y registro; pilares fundamentales del sistema de cadena de custodia.

"A pesar del escenario, la criminalística ofrece un espacio de análisis y estudio hacia una reflexión profunda sobre los hechos y las evidencias que se identifican en el lugar donde se llevaron a cabo las acciones catalogadas como criminales. En este momento, es preciso establecer un nuevo conjunto de herramientas, estrategias y acciones para descubrir en los medios informáticos, la evidencia digital que sustente y verifique las afirmaciones que sobre los hechos delictivos se han materializado en el caso bajo estudio". [20]

"Considerando la fragilidad de los elementos con el cual se trabaja en una escena, es preciso extremar las medidas de seguridad y control que éstos deben tener a la hora de adelantar sus labores, pues cualquier imprecisión en las mismas puede llevar a comprometer el proceso". [21]

El momento de la recolección es el procedimiento más crítico por lo que lo más importante es garantizar la autenticidad, pero para esto debe cumplir con lo siguiente:

- Demostrar que los elementos recolectados han sido obtenidos y registrados en el lugar de los hechos.
- Los elementos hallados no han sido alterados y/o modificados, o sea que corresponden a la realidad y que estos elementos no han sido eliminados, cambiados, aumentados, alterados, disminuidos de ninguna forma o bajo ningún proceso.

Teniendo en cuenta que un método es una secuencia que permite conseguir un fin, para evitar la contaminación o perdida de los elementos digitales hallados se debe tener en cuenta:

- Acordonar el lugar y aislar de todo campo magnético.
- No ingresar a la escena con ningún dispositivo electrónico o de comunicaciones, ya que puede alterar los elementos materiales probatorios y evidencias física de tipo digital que se van a recolectar.
- Proteger los equipos electrónicos de daños físicos.
- Proteger los datos contenidos dentro de los equipos electrónicos ya que pueden ser alterados por factores ambientales, magnéticos o electrónicos.
- Usar guantes antiestáticos y manillas antiestáticas
- Esterilidad (Borrado Seguro) de los insumos digitales con los cuales se va a realizar la recolección. Lo que permitirá tener la certeza que no van a permitir variación magnética en los datos y/o información recolectada.
- No encender los equipos o dispositivos electrónicos hallados.
- Si está encendido, no lo apague ya que se puede perder los datos volátiles. Aíslelo de cualquier alteración a los datos y/o información contenidos. En el evento que lo encuentre realizando algún borrado o destrucción de datos y/o información proceda apagarlo retirando la batería y desconectarlo del fluido eléctrico.
- No revisar ni manipular el dispositivo electrónico.
- Verificar si en las ranuras de almacenamiento removibles puedan estar insertadas tarjetas SD, Compact flash, Tarjetas XD, Memory Stick, etc.
- Sellar con cinta las ranuras de unidades de disco, puertos y tornillos, con esto se garantiza que no se va insertar ningún elemento al igual que no se ha cambiado nada del dispositivo.
- Usar bolsas especiales antiestáticas para almacenar los elementos recolectados (si no hay, utilizar papel). En todo caso NO utilizar bolsas plásticas, debido a que pueden ocasionar descargas de electricidad estática.
- En el momento de la recolección de los datos y/o información se debe verificar y actualizar los sistemas de antivirus y las actualizaciones de seguridad del equipo con el que se recolectan los elementos materiales probatorios y evidencia física.

Con esto se trata de dar a los jueces y fiscales elementos que deban tomar en consideración cuando un investigador les presente evidencia de naturaleza digital, de manera que estén en capacidad de decidir si la aceptan o la rechazan, dependiendo del nivel de certeza que alcancen respecto de si esa prueba ha sido modificada de alguna forma, en algún momento. El procedimiento forense digital busca precisamente evitar esas modificaciones de los datos contenidos en el medio magnético a analizar, que se pueden presentar en cualquier instante, desde el mismo momento en el que haya ocurrido el presunto hecho punible por razones tan diversas como el paso del tiempo, porque alguien haya decidido apagar la

máquina o por que se haya ejecutado en ella una aplicación que sobre escribió en la memoria, en fin.

También pueden presentarse como consecuencia de la intervención directa del investigador, cuya tarea inicial es preservar la evidencia y asegurarla, para posteriormente presentarla para su análisis. El aseguramiento se hace, única y exclusivamente, mediante la utilización de herramientas software y hardware que, a su vez, utilizan métodos matemáticos bastantes complejos para copiar cada medio magnético en forma idéntica; es decir, que les permiten obtener clones idénticos (copias iguales, *bit* a *bit*) al original. Cuando se presenta un delito informático, antes de analizar el hecho el investigador debe, inmediatamente, acordonar la escena, que puede no tener más de cinco centímetros de largo, si se trata de una memoria flash (del tipo USB); este acordonamiento de la escena no es otra cosa que clonar *bit* a *bit* los datos contenidos en ella. Así se obtiene una copia judicialmente aceptable no es tarea fácil; sin embargo, la industria, y la práctica legal en otros países, han definido estándares que, entre otros, se refieren a la necesidad de esterilizar el medio magnético en el que la copia será guardada; al paso a paso que debe seguir el investigador; a la aceptación que la comunidad científica da a los métodos matemáticos que están detrás de las herramientas hardware y software usadas por él; y, a la rata de error de esas herramientas. [22]

4.3. DISEÑAR Y NORMALIZAR LOS PROCEDIMIENTOS PARA LA RECOLECCIÓN, EMBALAJE Y EL TRATAMIENTO DE ELEMENTOS MATERIALES PROBATORIOS Y EVIDENCIA FÍSICA DE TIPO DIGITAL.

Respecto a los elementos digitales hallados en una escena se deben plantear procedimientos que permitan recolectarlos de la mejor manera para que conserven los principios de integridad, identidad y autenticidad. De esta manera se garantizaría que los elementos están recolectados correctamente y que al momento de realizar los respectivos estudios se va tener la certeza de que los datos y/o información contenida en ellos son los mismos que se encuentran en los dispositivos originales. Con éstos al momento de ser introducidos en juicio van a ser admitidos sin ninguna objeción en los estrados judiciales, garantizando confiabilidad e integridad de la evidencia.

“La recolección de evidencia informática es un aspecto frágil de la computación forense, especialmente porque requiere de prácticas y cuidados adicionales que no se tienen en la recolección de evidencia convencional. Es por esto que:

- Se debe proteger los equipos del daño.
- Se debe proteger la información contenida dentro de los sistemas de almacenamiento de información (muchas veces, estos pueden ser alterados fácilmente por causas ambientales, o por un simple campo magnético).

- Algunas veces, será imposible reconstruir la evidencia (o el equipo que la contiene), si no se tiene cuidado de recolectar todas las piezas que se necesiten". [23]

"Algo importante a la hora de recolectar evidencia, es la preservación de la integridad de ésta; en el caso particular de la información almacenada en medios magnéticos, la naturaleza volátil de ésta hace que dicha labor sea particularmente difícil. La primera gran decisión que se debe tomar a la hora de colectar evidencias, es la *cantidad* de ésta que se debe tomar. Un investigador podría estar tentado a llevarse todo el equipo que encuentre, para no arriesgarse a dejar piezas de información potencialmente importantes. Sin embargo, esta alternativa tiene sus inconvenientes, ya que el investigador podría terminar siendo demandado por dañar o alterar la vida de una persona o de un negocio más de lo absolutamente necesario. Desde este punto de vista, quizás lo indicado sería incautar sólo lo mínimo necesario para efectuar una investigación. Aunque en últimas, es la severidad y la categoría del crimen las que determinan cuánta evidencia digital se debe recolectar". [23]

Hay que tener en cuenta que los elementos recolectados pueden ser de la siguiente manera:

1.- Generados por el equipo y/o dispositivo
2.- Almacenados en el equipo y/o dispositivo

Para poder obtener estos elementos se deben tener en cuenta lo siguientes pasos de manera general:

- Se deben identificar los elementos a recolectar
- Revisar la política de utilización de los equipos y/o dispositivo para no ir en contra de la violación a la privacidad e intimidad
- Tener autorización para no infringir ninguna norma o derecho fundamental (Intimidad - Privacidad)
- Utilizar guantes antiestáticos y manillas antiestáticas
- Esterilizar los medios para la recolección de elementos digitales
- Documentar planimétricamente y fotográficamente en conjunto con todos los elementos conectados.
- Recolectar cables, fuentes de poder y otros dispositivos que estén conectados
- Documentar si se utilizó algún dispositivo adicional para realizar extracción de información
- Documentar hardware y software utilizado
- Recolectar los datos volátiles
- Generar Huella Hash
- Firmar digitalmente los elementos recolectados.
- Etiquetar los medios de recolección
- Recolectar, Embalar y Rotular los elementos

- Registrar fotográficamente todos los elementos recolectados

La figura a continuación se detalla a través de un diagrama general, donde se muestra cada uno de los pasos que deben tenerse en cuenta para llevar a cabo un adecuado tratamiento y recolección de datos e información que puedan hallarse en los dispositivos digitales que estén presentes en una escena.

DIAGRAMA GENERAL PARA LA RECOLECCION DE ELEMENTOS DIGITALES HALLADOS EN UNA ESCENA

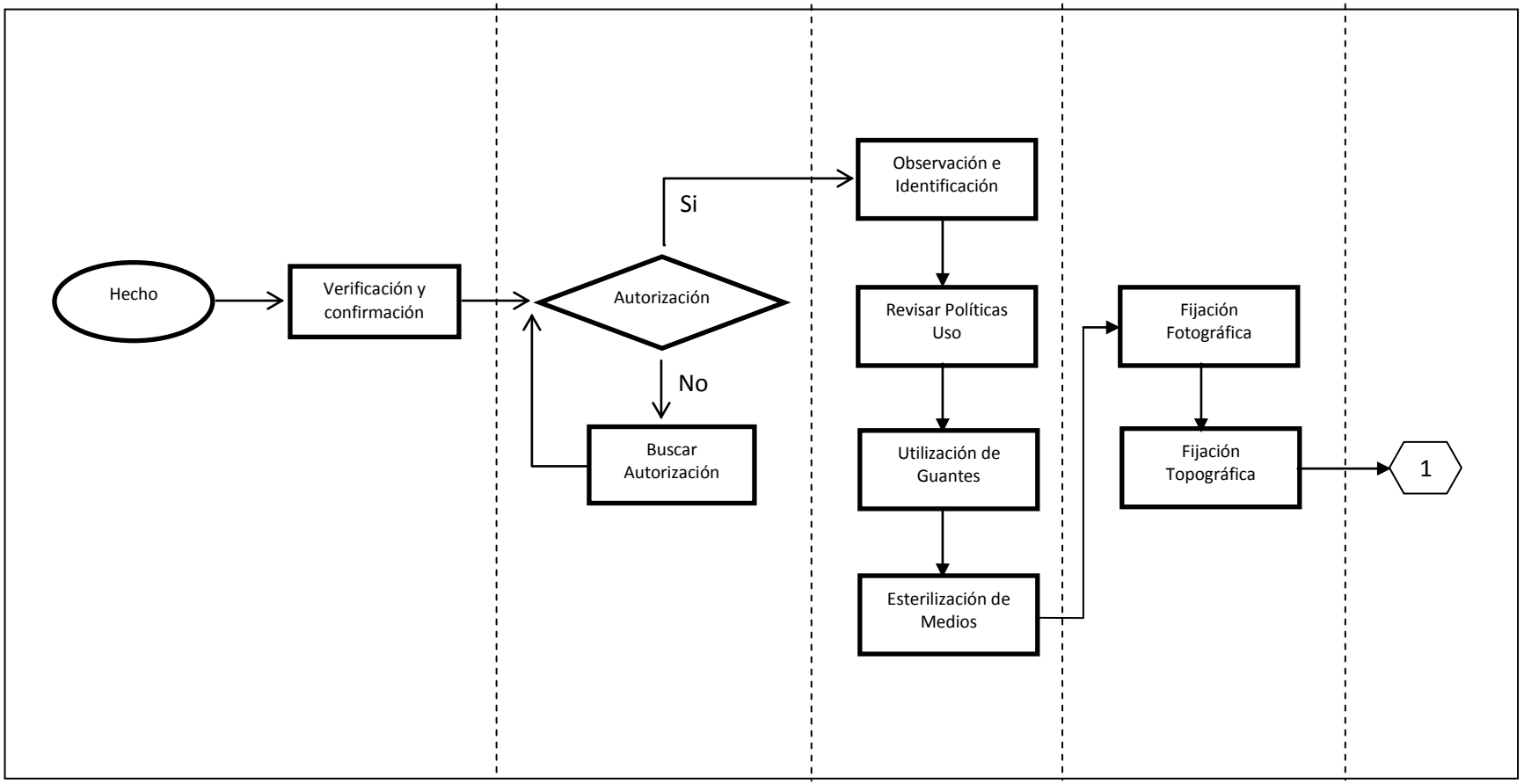
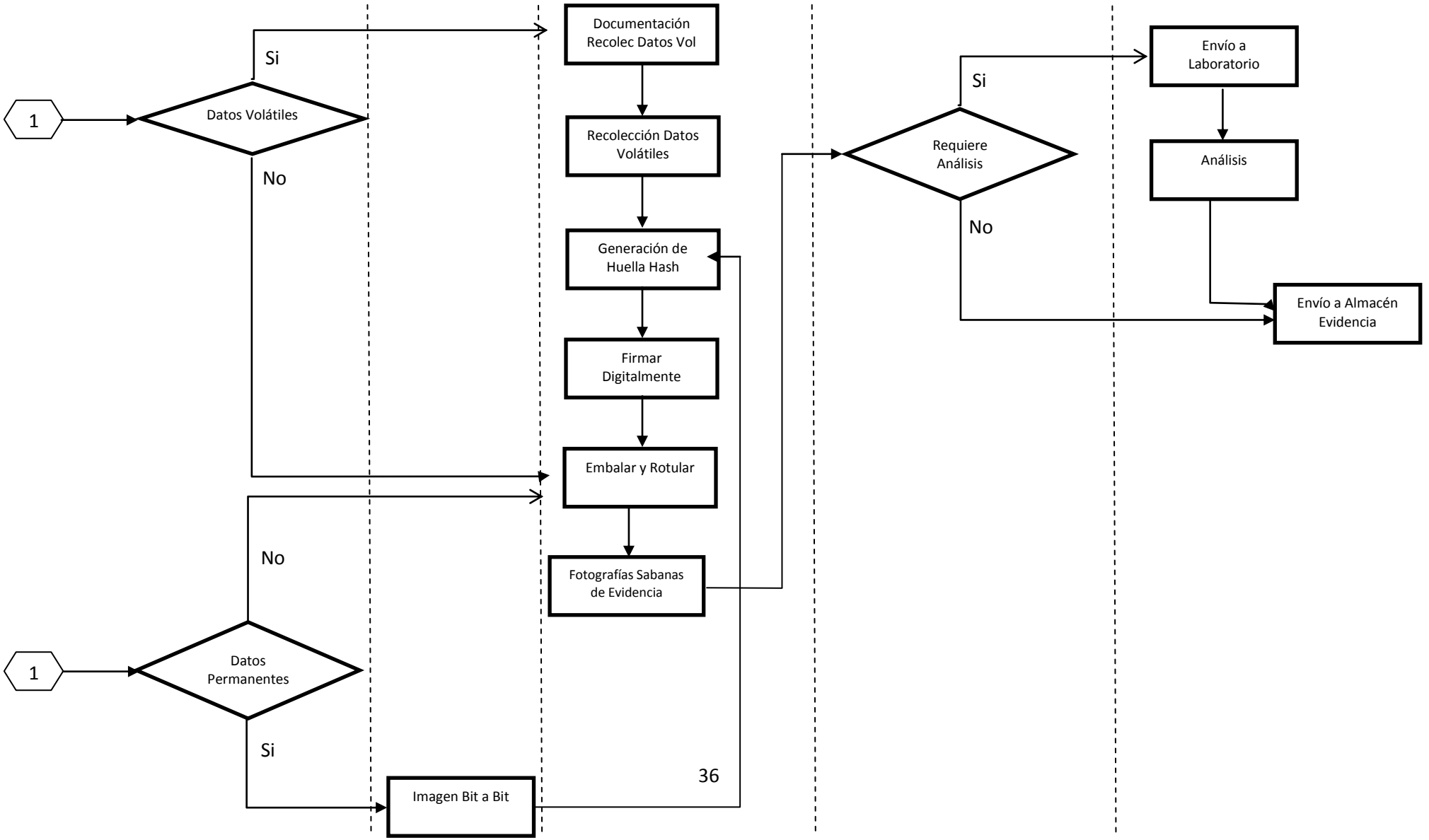


Figura No. 1. Diagrama general de recolección de elementos digitales


1
Datos Volátiles
Si
No
Documentación Recolec Datos Vol
Recolección Datos Volátiles
Generación de Huella Hash
Firmar Digitalmente
Embalar y Rotular
Fotografías Sabanas de Evidencia
Requiere Análisis
Si
No
Envío a Laboratorio
Análisis
Envío a Almacén Evidencia
1
Datos Permanentes
No
Si
Imagen Bit a Bit

Teniendo en cuenta que en una escena se puede obtener una variedad de elementos que contengan información digital se tiene una clasificación de acuerdo a su funcionalidad; por lo que, a continuación se detalla un procedimiento para cada uno de los ítems de la clasificación:

4.3.1 EQUIPOS DE CÓMPUTO

En este tipo de clasificación se tienen: ***Computador Portátil, Computador De Escritorio, Computador Tipo Servidor, Tablet PC***. Debido a su funcionalidad y tipo de datos e información almacenada se realiza el siguiente procedimiento para realizar la recolección:

Si el Equipo de Cómputo se encuentra encendido:

1.- Mover el mouse para evitar bloqueos y verificar el estado de las baterías
2.- Recolectar Datos Volátiles
3.- Apagar abruptamente y/o retirar la batería
4.- Identificar los dispositivos de Almacenamiento (Discos Duros, memorias extraíbles, otros)
5.- Extraer los dispositivos de almacenamiento instalados
6.- Instalar y conectar bloqueadores contra escritura
7.- Documentar Fotográficamente los equipos instalados y Print Screen del procedimiento de la imagen forense
8.- Realizar imagen forense Bit a Bit
9.- Generar Huella Hash
10.- Verificar la imagen forense realizada
11.- Firmar digitalmente la imagen realizada
12.- Cifrarlo y guardarlo en dispositivos de solo lectura
13.- Etiquetar, embalar y rotular los elementos hallados

Si el Equipo de Cómputo se encuentra apagado:

1.- Identificar los dispositivos de Almacenamiento (Discos Duros, memorias extraíbles, otros)
2.- Extraer dispositivos de almacenamiento instalados
3.- Instalar y conectar bloqueadores contra escritura
4.- Documentar Fotográficamente los equipos instalados y Print Screen del procedimiento de la imagen forense
5.- Realizar imagen forense Bit a Bit
6.- Generar Huella Hash
7.- Verificar la imagen forense realizada
8.- Firmar digitalmente la imagen realizada
9.- Cifrarlo y guardarlo en dispositivos de solo lectura
10.- Etiquetar, embalar y rotular los elementos hallados

DIAGRAMA PARA LA RECOLECCION DE EQUIPOS DE COMPUTOS

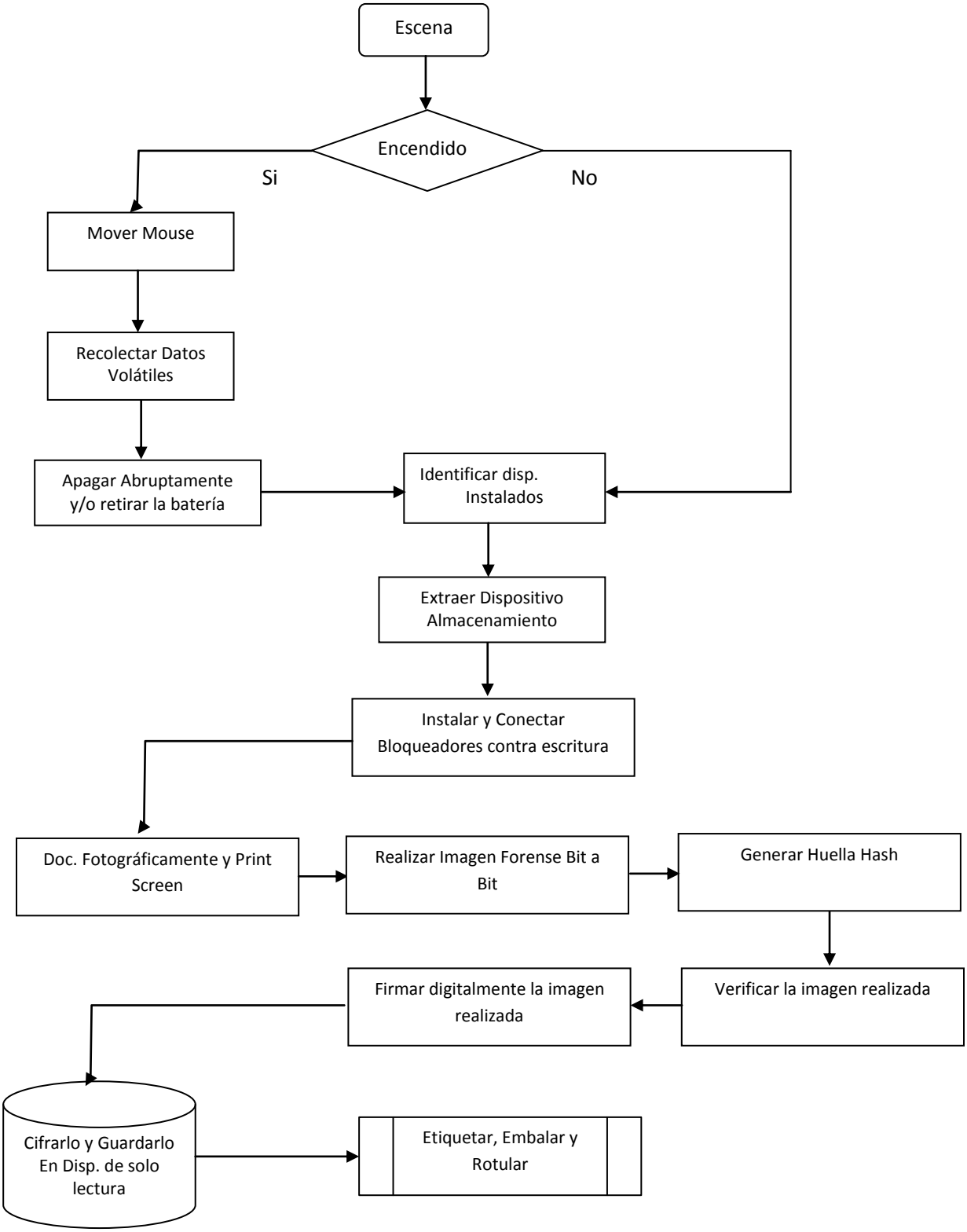


Figura No. 2. Diagrama de recolección de equipos de cómputos

4.3.2 DISPOSITIVOS DE COMUNICACIÓN DE DATOS

En este tipo de clasificación se tienen: ***Router, Firewall, entre otros***. Debido a su funcionalidad y tipo de datos e información almacenada se realiza el siguiente procedimiento para realizar la recolección:

Si el Dispositivo de Comunicación de Datos se encuentra encendido:

1.- Recolectar Datos Volátiles
2.- Apagar abruptamente
3.- Extraer dispositivos de almacenamiento instalados
4.- Instalar y conectar bloqueadores contra escritura
5.- Documentar Fotográficamente los equipos instalados y Print Screen del procedimiento de la imagen forense
6.- Realizar imagen forense Bit a Bit
7.- Generar Huella Hash
8.- Verificar la imagen forense realizada
9.- Firmar digitalmente la imagen realizada
10.- Cifrarlo y guardarlo en dispositivos de solo lectura
11.- Etiquetar, embalar y rotular los elementos hallados

Si el Dispositivo de Comunicación de Datos se encuentra apagado:

1.- Extraer dispositivos de almacenamiento instalados
2.- Instalar y conectar bloqueadores contra escritura
3.- Documentar Fotográficamente los equipos instalados y Print Screen del procedimiento de la imagen forense
4.- Realizar imagen forense Bit a Bit
5.- Generar Huella Hash
6.- Verificar la imagen forense realizada
7.- Firmar digitalmente la imagen realizada
8.- Cifrarlo y guardarlo en dispositivos de solo lectura
9.- Etiquetar, embalar y rotular los elementos hallados

DIAGRAMA PARA LA RECOLECCION DE DISPOSITIVOS DE COMUNICACIÓN DE DATOS

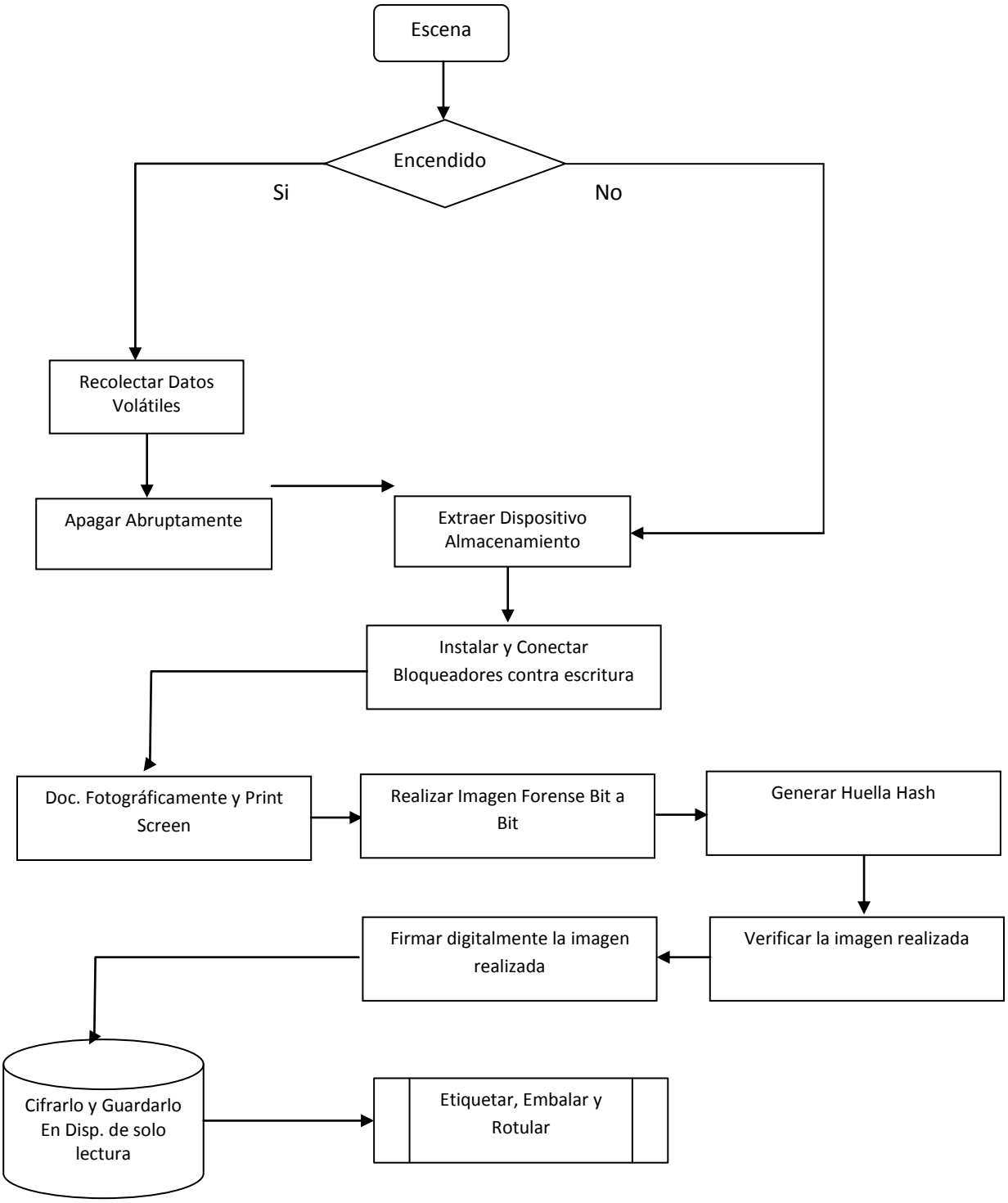


Figura No. 3. Diagrama de recolección de dispositivos de comunicación de datos

4.3.3 DISPOSITIVOS DE CAPTURA DE DATOS, AUDIOS E IMÁGENES

En este tipo de clasificación se tienen: ***DVR, Grabadoras Digitales, Reproductores MP3, MP4, MP5, Cámaras Fotográficas, Cámaras de Video***. Debido a su funcionalidad y tipo de datos e información almacenada se realiza el siguiente procedimiento para realizar la recolección:

Si el Dispositivo se encuentra encendido:

1.- Apagar el dispositivo
2.- Extraer Batería y/o dispositivo de alimentación de energía
3.- Extraer dispositivos de almacenamiento instalados
4.- Instalar y conectar bloqueadores contra escritura
5.- Documentar Fotográficamente los equipos instalados y Print Screen del procedimiento de la imagen forense
6.- Realizar imagen forense Bit a Bit
7.- Generar Huella Hash
8.- Verificar la imagen forense realizada
9.- Firmar digitalmente la imagen realizada
10.- Cifrarlo y guardarlo en dispositivos de solo lectura
11.- Etiquetar, embalar y rotular los elementos hallados

Si el Dispositivo se encuentra apagado:

1.- Extraer Batería y/o dispositivo de alimentación de energía
2.- Extraer dispositivos de almacenamiento instalados
3.- Instalar y conectar bloqueadores contra escritura
4.- Documentar Fotográficamente los equipos instalados y Print Screen del procedimiento de la imagen forense
5.- Realizar imagen forense Bit a Bit
6.- Generar Huella Hash
7.- Verificar la imagen forense realizada
8.- Firmar digitalmente la imagen realizada
9.- Cifrarlo y guardarlo en dispositivos de solo lectura
10.- Etiquetar, embalar y rotular los elementos hallados

DIAGRAMA PARA LA RECOLECCION DE DISPOSTIVOS DE CAPTURA DE DATOS, AUDIOS E IMAGENES

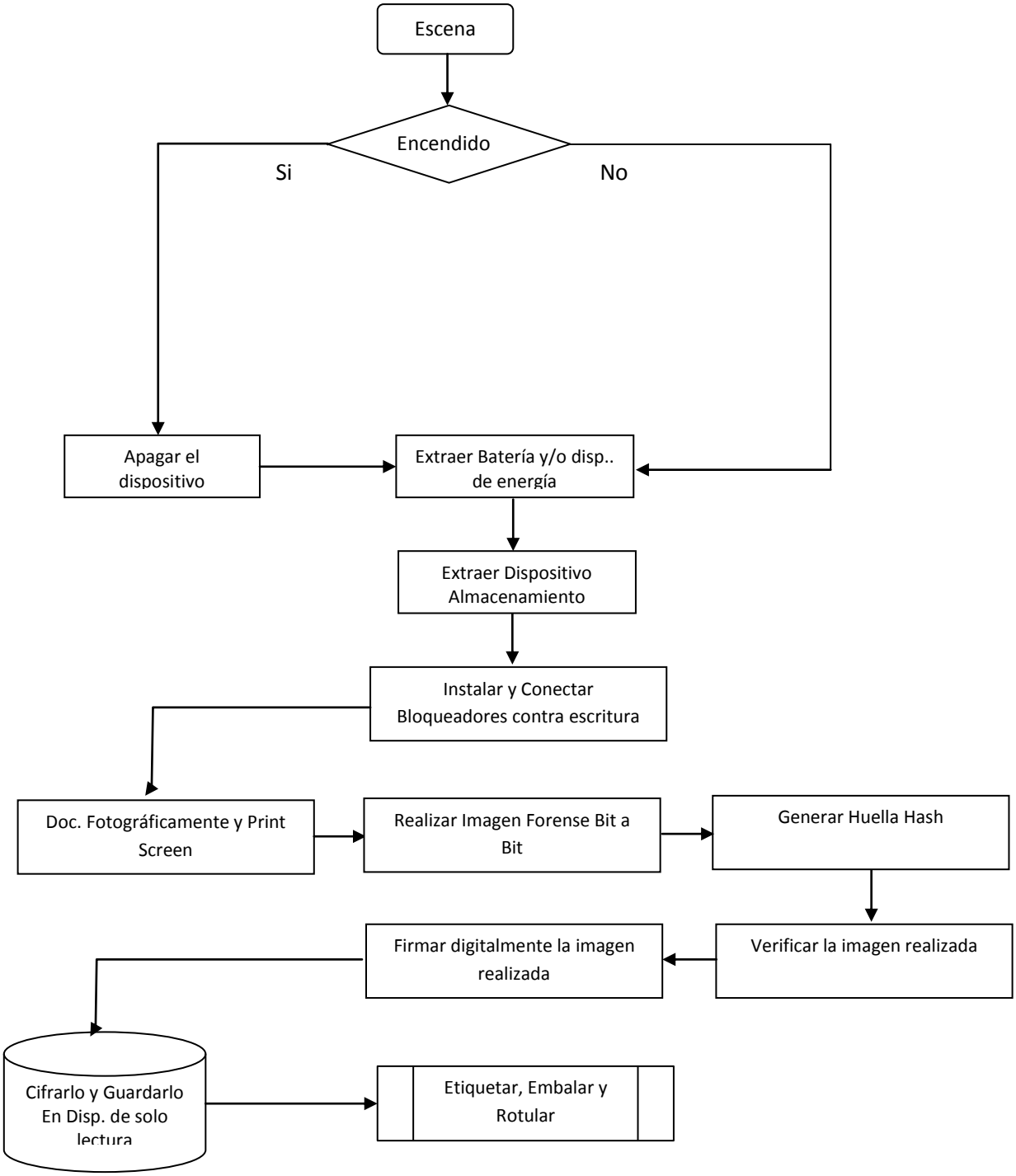


Figura No. 4. Diagrama de recolección de dispositivos de captura de datos, audios e imágenes

4.3.4 EQUIPOS DE COMUNICACIÓN

En este tipo de clasificación se tienen: ***Teléfonos Celulares, IPod – IPad, IPhone, Palm – Pocket – PDA***. Debido a su funcionalidad y tipo de datos e información almacenada se realiza el siguiente procedimiento para realizar la recolección:

Si el Equipo de Comunicación se encuentra encendido:

1.- Bloquear las señales
2.- Generar el No. IMEI (* # 06 #) para identificarlo
3.- Introducirlo de frente en una bolsa de Faraday, bolsa antiestática o envolverlo en papel y después papel aluminio para aislar las señales
4.- Conectarlo al equipo forense para dispositivos móviles por si tiene clave
5.- Extraer la batería y la sim card
6.- Clonar la tarjeta sim card
7.- Realizar imagen forense
8.- Realizar extracción de datos del teléfono y sim card
9.- Firmar digitalmente los datos extraídos y la imagen realizada
10.- Cifrarlo y guardarlo en dispositivos de solo lectura
11.- Etiquetar, embalar y rotular los elementos hallados

Si el Equipo de Comunicación se encuentra apagado:

1.- Introducirlo de frente en una bolsa de Faraday, bolsa antiestática y/o papel aluminio para aislar las señales
2.- Extraer la batería y la sim card
3.- Clonar la tarjeta sim card
4.- Realizar imagen forense y huella hash
5.- Realizar extracción de datos del teléfono y sim card
6.- Firmar digitalmente los datos extraídos y la imagen realizada
7.- Cifrarlo y guardarlo en dispositivos de solo lectura
8.- Etiquetar, embalar y rotular los elementos hallados

DIAGRAMA PARA LA RECOLECCION DE EQUIPOS DE COMUNICACION

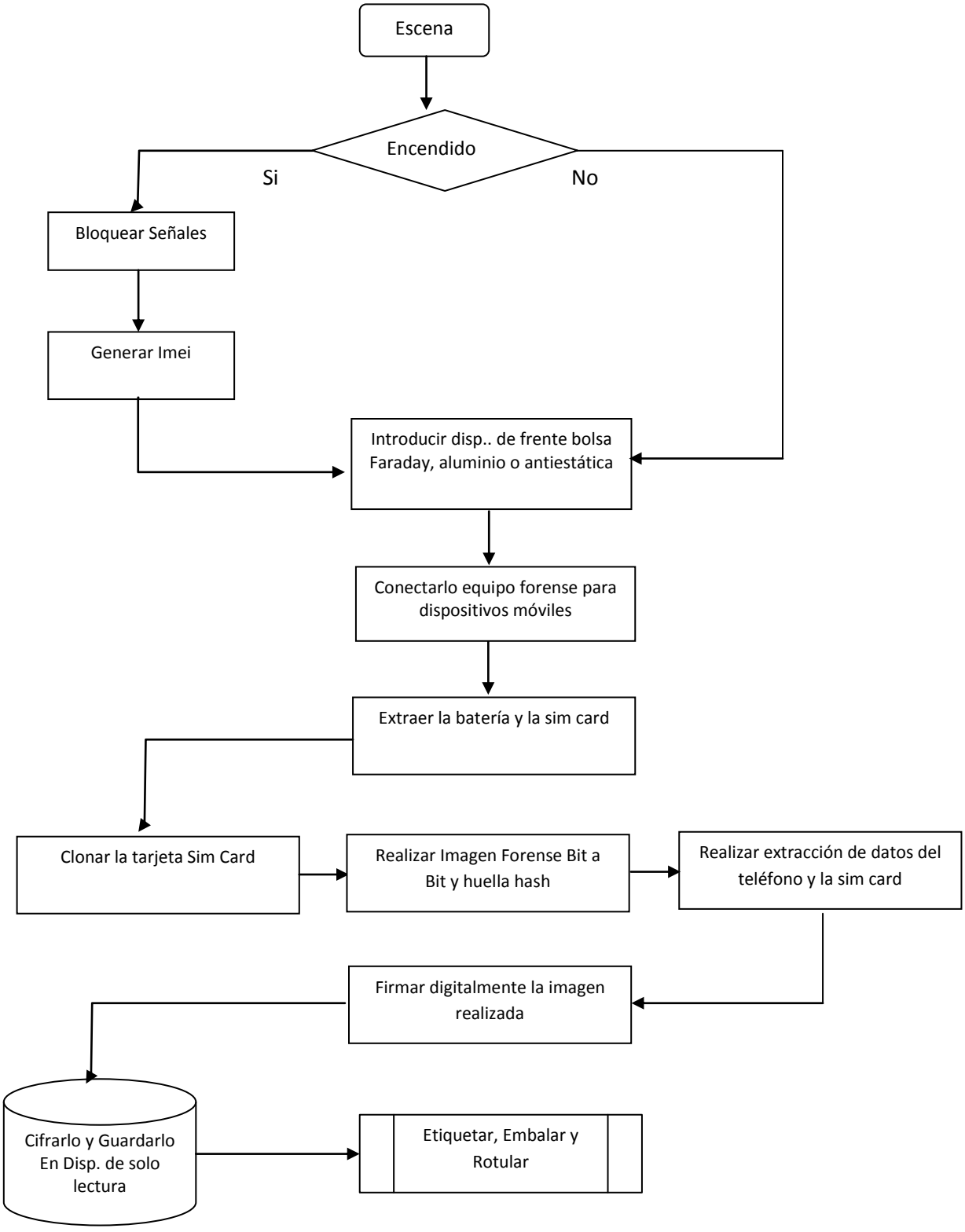


Figura No. 5. Diagrama de recolección de equipos de comunicación

4.3.5 SISTEMAS DE ALMACENAMIENTO - A gran escala

En este tipo de clasificación se tienen: ***Sistemas de Discos Raid – Arreglo de Discos, Sistemas SAN – Clúster***. Debido a su funcionalidad y tipo de datos e información almacenada se realiza el siguiente procedimiento para realizar la recolección:

Si el Sistema de Almacenamiento – A gran escala se encuentra encendido:

1.- Mover el mouse para evitar bloqueos
2.- Recolectar datos volátiles y apagar si se puede
3.- Iniciar software forense de recolección de información para sistemas en vivo (Ej. Hélix)
4.- Documentar fotográficamente la pantalla y Print Screen del procedimiento forense
5.- Realizar imagen forense Bit a Bit
6.- Generar Huella Hash
7.- Verificar la imagen forense realizada
8.- Firmar digitalmente la imagen realizada
9.- Cifrarlo y guardarlo en dispositivos de solo lectura
10.- Etiquetar, embalar y rotular los elementos hallados

Si el Sistema de Almacenamiento – A gran escala se encuentra apagado:

1.- Identificar los dispositivos de Almacenamiento (Discos Duros)
2.- Extraer dispositivos de almacenamiento instalados
3.- Instalar y conectar bloqueadores contra escritura y/o virtualizar y extraer con software forense de recolección de información para sistemas en vivo (Ej. Hélix)
4.- Documentar Fotográficamente la pantalla y Print Screen del procedimiento de la imagen forense
5.- Realizar imagen forense Bit a Bit
6.- Generar Huella Hash
7.- Verificar la imagen forense realizada
8.- Firmar digitalmente la imagen realizada
9.- Cifrarlo y guardarlo en dispositivos de solo lectura
10.- Etiquetar, embalar y rotular los elementos hallados

DIAGRAMA PARA LA RECOLECCION DE SISTEMAS DE ALMACENAMIENTO – A GRAN ESCALA

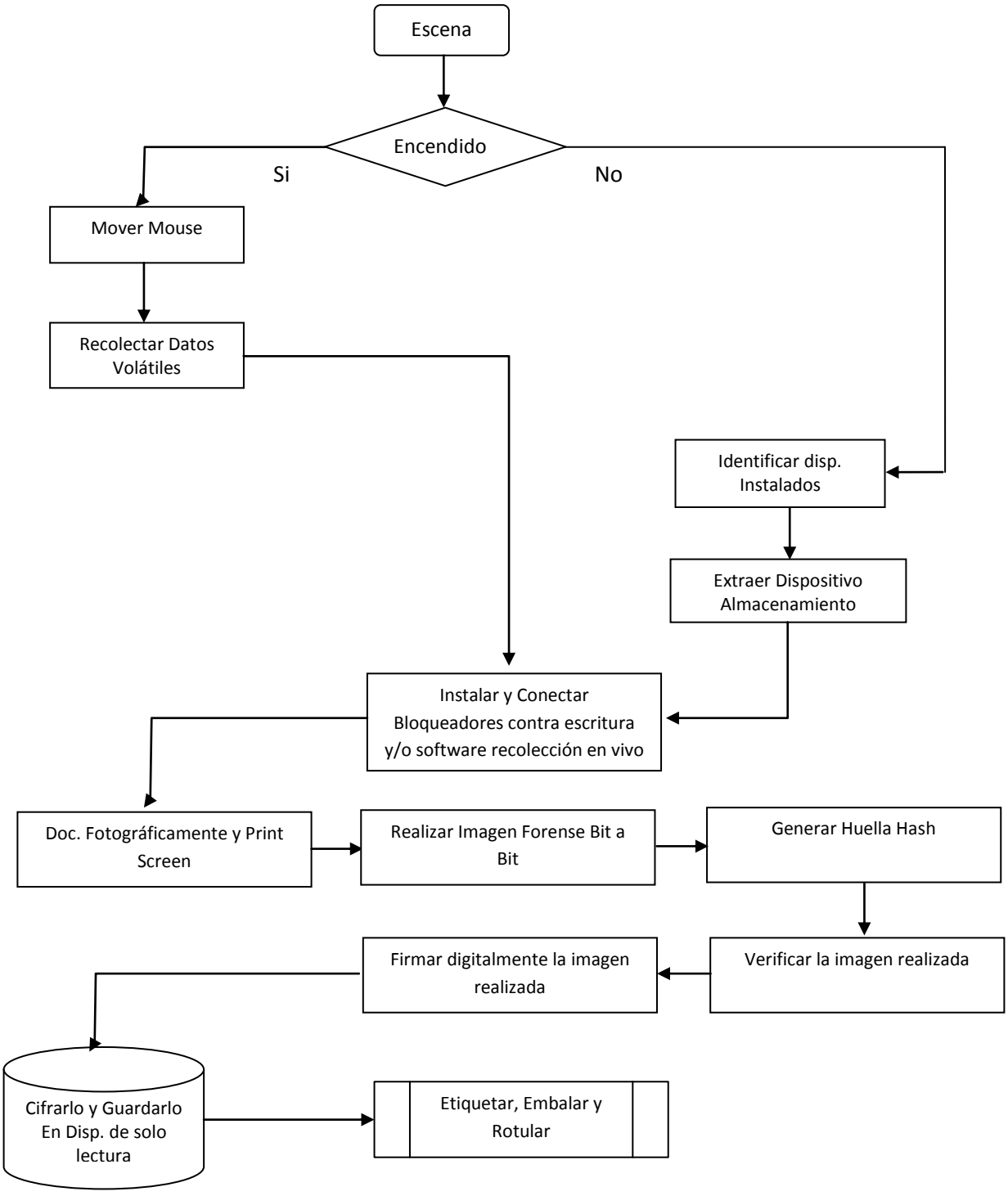


Figura No. 6. Diagrama de recolección de sistemas de almacenamiento – a gran escala

4.3.6 SISTEMAS DE ALMACENAMIENTO – Portable

En este tipo de clasificación se tienen: ***CD - DVD, Duplicadora de Discos, Diskettes, Discos Duros (IDE – ATA – SATA - SCSI), Discos Duros Externos, Micro Drive, Cintas Magnéticas, Discos ZIP, Memorias USB, Memorias (SD – Micro SD – MMC – XD), Sim Card de Teléfonos Móviles Celulares***. Debido a su funcionalidad y tipo de datos e información almacenada se realiza el siguiente procedimiento para realizar la recolección:

Si el Sistema de Almacenamiento – Portable

1.- Identificar los dispositivos de Almacenamiento (Discos Duros, memorias extraíbles, otros)
2.- Extraer dispositivos de almacenamiento instalados
3.- Instalar y conectar bloqueadores contra escritura
4.- Documentar Fotográficamente los equipos instalados y Print Screen del procedimiento de la imagen forense
5.- Realizar imagen forense Bit a Bit
6.- Generar Huella Hash
7.- Verificar la imagen forense realizada
8.- Firmar digitalmente la imagen realizada
9.- Cifrarlo y guardarlo en dispositivos de solo lectura
10.- Etiquetar, embalar y rotular los elementos hallados

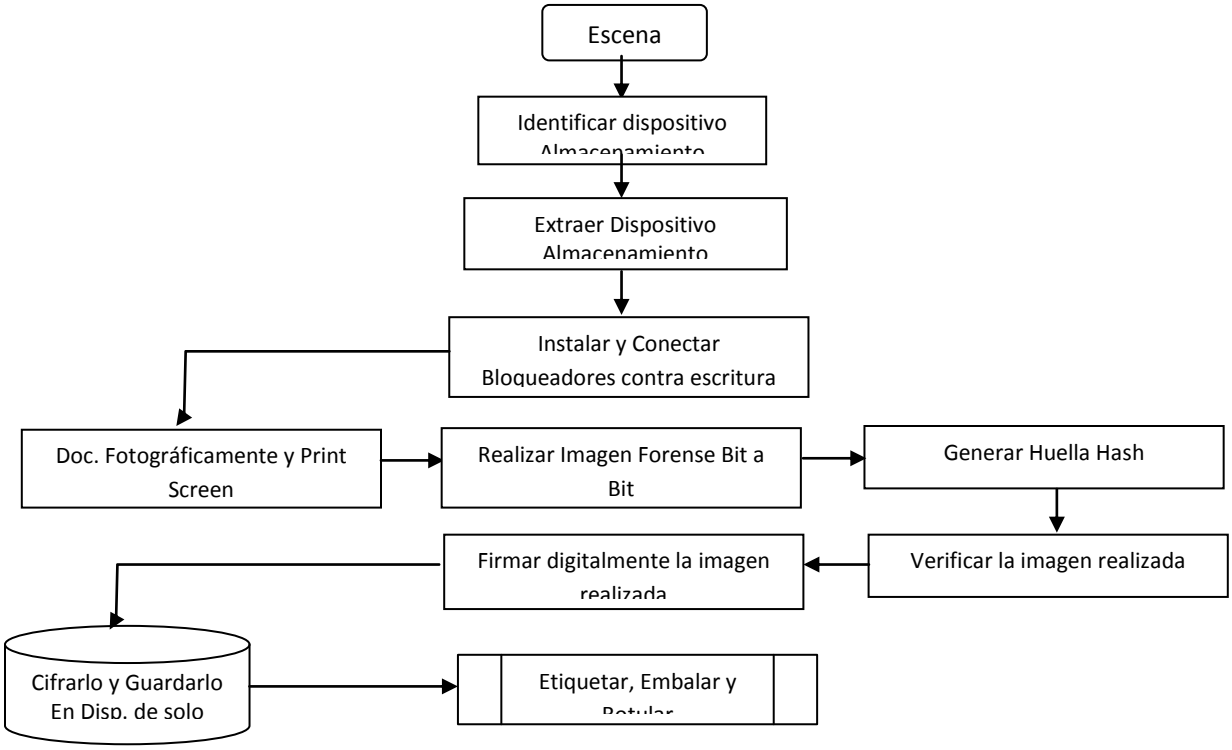


Figura No. 7. Diagrama de recolección de sistemas de almacenamiento - portable

4.3.7 SISTEMAS DE IMPRESIÓN

En este tipo de clasificación se tienen: ***Copiadoras – Fotocopiadoras, Impresoras, Fax.*** Debido a su funcionalidad y tipo de datos e información almacenada se realiza el siguiente procedimiento para realizar la recolección:

En el Sistema de Impresión:

1.- Desconectarlo de la red de datos y voz
2.- Recolectar Datos Volátiles
3.- Generar logs y/o registros
4.- Apagar abruptamente y/o retirar la batería
5.- Generar Huella Hash de los datos volátiles
6.- Firmar digitalmente la imagen realizada
7.- Cifrarlo y guardarlo en dispositivos de solo lectura
8.- Etiquetar, embalar y rotular los elementos hallados

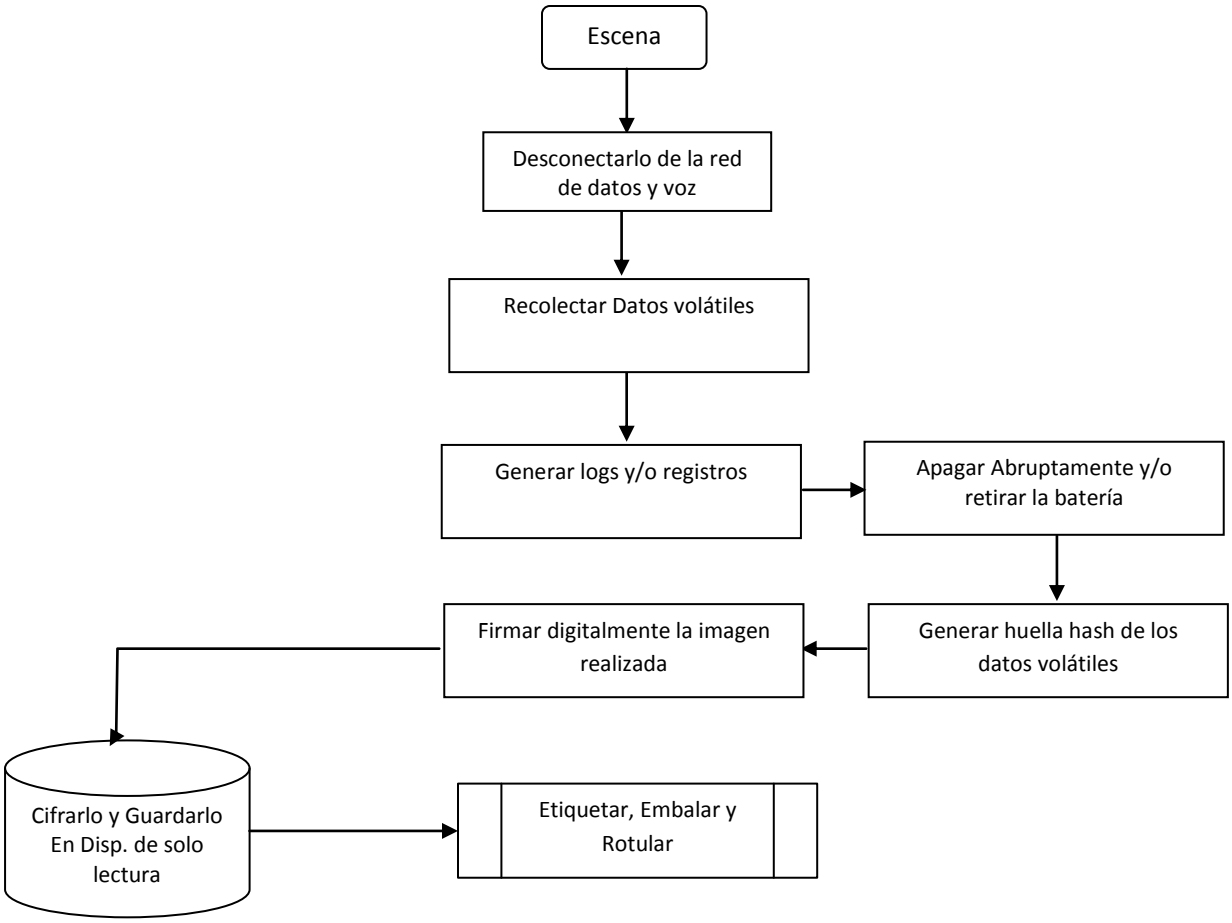


Figura No. 8. Diagrama de recolección de sistemas de impresión

4.3.8 OTROS DISPOSITIVOS

En este tipo de clasificación se tienen: ***GPS, Juegos Electrónicos – X box.*** Debido a su funcionalidad y tipo de datos e información almacenada se realiza el siguiente procedimiento para realizar la recolección:

Si el Dispositivo se encuentra encendido:

1.- Apagar el dispositivo
2.- Extraer Batería y/o dispositivo de alimentación de energía
3.- Extraer dispositivos de almacenamiento instalados
4.- Instalar y conectar bloqueadores contra escritura
5.- Documentar Fotográficamente los equipos instalados y Print Screen del procedimiento de la imagen forense
6.- Realizar imagen forense Bit a Bit
7.- Generar Huella Hash
8.- Verificar la imagen forense realizada
9.- Firmar digitalmente la imagen realizada
10.- Cifrarlo y guardarlo en dispositivos de solo lectura
11.- Etiquetar, embalar y rotular los elementos hallados

Si el Dispositivo se encuentra apagado:

1.- Extraer Batería y/o dispositivo de alimentación de energía
2.- Extraer dispositivos de almacenamiento instalados
3.- Instalar y conectar bloqueadores contra escritura
4.- Documentar Fotográficamente los equipos instalados y Print Screen del procedimiento de la imagen forense
5.- Realizar imagen forense Bit a Bit
6.- Generar Huella Hash
7.- Verificar la imagen forense realizada
8.- Firmar digitalmente la imagen realizada
9.- Cifrarlo y guardarlo en dispositivos de solo lectura
10.- Etiquetar, embalar y rotular los elementos hallados

DIAGRAMA PARA LA RECOLECCION DE OTROS DISPOSITIVOS

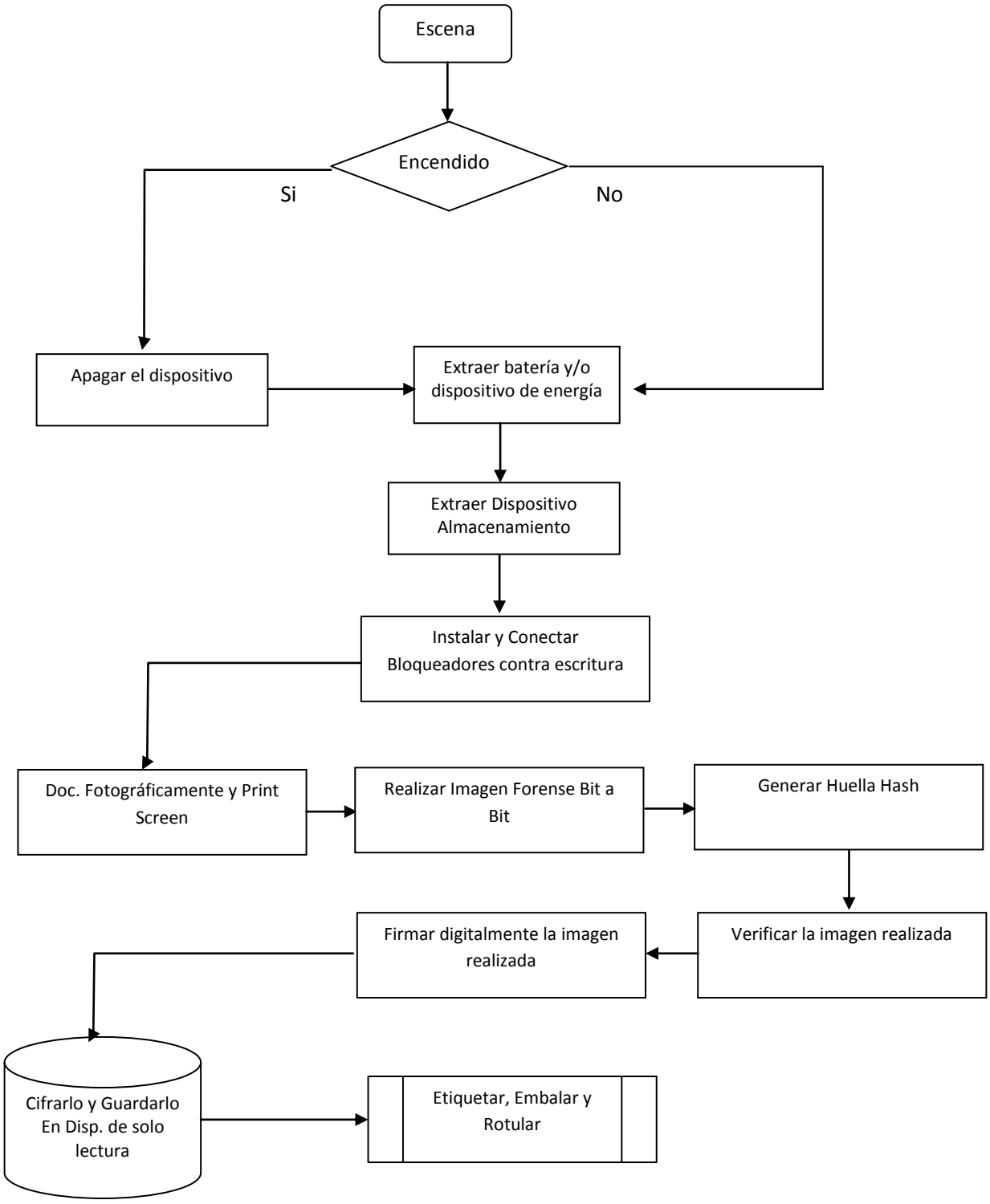


Figura No. 9. Diagrama de recolección de otros dispositivos

4.4. ELEMENTOS APROPIADOS PARA EL EMBALAJE Y ALMACENAMIENTO DE LOS ELEMENTOS MATERIALES PROBATORIOS Y EVIDENCIA FÍSICA DE TIPO DIGITAL.

Para garantizar la integridad y valor probatorio de los elementos digitales dentro de un juicio obteniendo la admisibilidad, no solo debe evitarse la contaminación tanto en la identificación y la recolección, sino también debe valorarse los elementos en los cuales son embalados, por lo que en esta etapa pueden influir factores ambientales y ajenos a los mismos elementos que puedan interferir y garantizar una confiabilidad total para demostrar que se ha conservado los pilares fundamentales del sistema de cadena de custodia como son de integridad, identidad y autenticidad.

Para el embalaje de los elementos materiales probatorios y evidencia física de tipo digital se debe tener en cuenta lo siguientes elementos así:

- **EQUIPOS DE CÓMPUTO**

En este tipo de clasificación se tienen: ***Computador Portátil, Computador De Escritorio, Computador Tipo Servidor, Tablet PC***.

1.- Esponja poliuretano antiestático
2.- Bolsa de burbuja antiestática
3.- Caja de cartón con recubrimiento antiestático.

En caso de no tener estos elementos se puede realizar lo siguiente:

1.- Esponja o bolsa de papel
2.- Bolsa antiestática
3.- Caja de cartón

- **DISPOSITIVOS DE COMUNICACIÓN DE DATOS**

En este tipo de clasificación se tienen: ***Router, Firewall, VPN****.*

1.- Esponja poliuretano antiestático
2.- Bolsa de burbuja antiestática
3.- Caja de cartón con recubrimiento antiestático.

En caso de no tener estos elementos se puede realizar lo siguiente:

1.- Esponja o bolsa de papel
2.- Bolsa antiestática
3.- Caja de cartón

- **DISPOSITIVOS DE CAPTURA DE DATOS, AUDIOS E IMÁGENES**

En este tipo de clasificación se tienen: ***DVR, Grabadoras Digitales, Reproductores MP3, MP4, MP5, Cámaras Fotográficas, Cámaras de Video***.

1.- Esponja poliuretano antiestático
2.- Bolsa de burbuja antiestática
3.- Caja de cartón con recubrimiento antiestático.
4.- Bolsa de papel
5.- Bolsa antiestática

En caso de no tener estos elementos se puede realizar lo siguiente:

1.- Esponja convencional y/o cartón doblado.
2.- Bolsa de papel y/o papel
3.- Bolsa antiestática y/o papel aluminio
4.- Bolsa plástica
5.- Caja de cartón

- **EQUIPOS DE COMUNICACIÓN**

En este tipo de clasificación se tienen: ***Teléfonos Celulares, IPod – IPad, IPhone, Palm – Pocket – PDA***.

1.- Esponja poliuretano antiestático
2.- Bolsa de burbuja antiestática
3.- Bolsa Faraday, antiestática y/o papel aluminio

En caso de no tener estos elementos se puede realizar lo siguiente:

1.- Esponja o bolsa de papel
2.- Bolsa antiestática y/o papel aluminio

- **SISTEMAS DE ALMACENAMIENTO - A gran escala**

En este tipo de clasificación se tienen: ***Sistemas de Discos Raid – Arreglo de Discos, Sistemas SAN – Clúster***.
1.- Esponja poliuretano antiestático
2.- Bolsa de burbuja antiestática
3.- Caja de cartón con recubrimiento antiestático.

En caso de no tener estos elementos se puede realizar lo siguiente:

1.- Esponja o bolsa de papel
2.- Bolsa antiestática
3.- Caja de cartón

- **SISTEMAS DE ALMACENAMIENTO – Portable**

En este tipo de clasificación se tienen: ***CD - DVD, Duplicadora de Discos, Diskettes, Discos Duros (IDE – ATA – SATA - SCSI), Discos Duros Externos, Micro Drive, Cintas Magnéticas, Discos ZIP, Memorias USB, Memorias (SD – Micro SD – MMC – XD), Sim Card de Teléfonos Móviles Celulares***.

1.- Bolsa de papel
2.- Bolsa antiestática

En caso de no tener estos elementos se puede realizar lo siguiente:

1.- Bolsa de papel y/o papel
2.- Bolsa antiestática y/o papel aluminio
3.- Bolsa plástica

- **SISTEMAS DE IMPRESIÓN**

En este tipo de clasificación se tienen: ***Copiadoras – Fotocopiadoras, Impresoras, Fax.***

1.- Esponja poliuretano antiestático
2.- Bolsa de burbuja antiestática
3.- Caja de cartón con recubrimiento antiestático.

En caso de no tener estos elementos se puede realizar lo siguiente:

1.- Esponja o bolsa de papel
2.- Bolsa antiestática
3.- Caja de cartón

- **OTROS**

En este tipo de clasificación se tienen: ***GPS, Juegos Electrónicos – X box***.

1.- Esponja poliuretano antiestático

2.- Bolsa de burbuja antiestática
3.- Caja de cartón con recubrimiento antiestático.

En caso de no tener estos elementos se puede realizar lo siguiente:

1.- Esponja o bolsa de papel
2.- Bolsa antiestática
3.- Caja de cartón

Para tener en cuenta que los elementos de tipo digitales se deben embalar separadamente y no se permiten colocarle rótulos o adhesivo directamente sobre la superficie, así como tampoco escribir encima de ellos. Adicionalmente estos elementos requieren ser almacenados en lugares libre de humedad y campo electromagnético.

5. CONCLUSIONES

Se logró establecer que existen diversos factores tales como ambientales, electrónicos, eléctricos, que al no mitigarlos adecuadamente inciden de manera directa en las evidencias de tipo digital alterándolos y generando una pérdida sustancial de datos y/o información.

La manipulación no adecuada de las evidencias digitales en una escena pueden perderse y/o contaminarse debido a su fragilidad y volatilidad.

Con la exposición de los datos volátiles a la recolección no adecuada se puede perder información valiosa y que al intentar una reconstrucción de la escena para poder llevar a cabo un análisis adecuado, se puede generar una interpretación inadecuada de como se comportaba la escena al momento de la recolección de datos.

Con las características que tiene los elementos de embalaje de las evidencias digitales, ayudan a mitigar y proteger las evidencias de cualquier alteración, modificación, contaminación o destrucción.

La orientación de que tipos de elementos pueden contener datos y/o información de tipo digital es una gran ayuda para los investigadores que procesan escena y lugar de los hechos, debido a que dependiendo del delito se puede inferir lógicamente que elementos son relevantes para la investigación.

Hemos obtenido un prototipo para el Cuerpo Técnico de Investigación – C.T.I. que ayuda de manera sustancial en el manejo de las escena donde se encuentren elementos digitales

Se logró establecer que existen diversos factores tales como ambientales, electrónicos, eléctricos, que al no mitigarlos altera los elementos digitales.

El protocolo realizado trata de garantizar de que no ocurra manipulación inadecuada que permita la pérdida de información

Nuestro protocolo ha tenido en cuenta la volatilidad de los elementos de le evidencia al momento de la recolección y así evitar perder información valiosa.

El protocolo tiene en cuenta que los elementos de embalaje ayudan a mitigar cualquier alteración, modificación, contaminación o destrucción del elemento.

El protocolo realizado es el punto de partida para un posterior trabajo que requiere labores de campo más amplios y estudios mas profundos.

6. RECOMENDACIONES

Los sistemas computacionales son sensibles a la temperatura, la humedad, choques físicos, electricidad estática y fuerzas electromagnéticas, por lo que deben ser tomadas las medidas de protección necesarias como manillas antiestáticas, retirar joyas antes y utilizar guantes.

Evitar dejar estos elementos en vehículos por tiempo prolongado.

Protegerlos de golpes físicos.

Evitar doblar, plegar o rayar los medios electrónicos como Discos duros, Cds, DvDs, cintas, USB, etc

Para el transporte de elementos de tipo digital, deben tenerse en cuenta recomendaciones de fragilidad, alejarlos de fuentes de energía, equipos de rayos X etc.

REFERENCIAS BIBLIOGRAFICAS

[1] Admin. (2009). Delincuencia Informática en Colombia. [En Línea] Disponible: http://www.atlas.com.co/webatlas/sia_blog/?p=497.

[2] Ley 1273 de 2009 – Ley de delitos informáticos

[3] F. Bautista. (2010). Aumentos de delitos en la internet [En línea] Disponible: http://www.delitosinformaticos.gov.co/node/5.

[4] A. Díaz García. (2011). Aniversario de la ley de delitos informáticos en Colombia. [En línea]. Disponible: http://www.slideshare.net/Alediaganet/aniversario-de-la-ley-de-delitos-informticos-en-colombia.

[5] http://fgn.fiscalia.gov.co/Fiscalia/contenido/html/Entidad.jsp [En línea].

[6] http://fgn.fiscalia.gov.co/Fiscalia/contenido/html/informacionPenal.jsp [En línea].

[7] G. Zuccardi, J.D. Gutiérrez. (2006). Infraestructura para la gestión de la evidencia digital en redes inalámbricas. [En línea]. Disponible:http://pegasus.javeriana.edu.co/~edigital/Docs/PropuestaII_v1.5.pdf.

[8] G. Zuccardi, J.D. Gutiérrez. (2006). Informática Forense. [En línea]. Disponible:http://pegasus.javeriana.edu.co/~edigital/Docs/Informatica%20Forense/Informatica%20Forense%20v0.6.pdf.

[9] V. Cobarrubias. (2008). Protocolo informático forense 7 fases. [En línea]. Disponible: http://forenseinformatico.blogspot.com/.

[10] Casey, Eoghan. “Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet”. 2004.

[11] J. Cano. Computación Forense – Descubriendo los rastros informáticos, Ed. Alfaomega, 2009.

[12] Manual Único de Policía Judicial, Fiscalía General de la Nación – Colombia, 2008.

[13] Manual Único de Cadena de Custodia, Fiscalía General de la Nación – Colombia, 2008.

[14] Ley 1273 de 2009 – Congreso de la Republica, http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html [En línea].

[15] Ley 1266 de 2008 – Congreso de la Republica, http://www.secretariasenado.gov.co/senado/basedoc/ley/2008/ley_1266_2008.html [En línea].

[16] Ley 906 de 2004 – Congreso de la Republica, http://www.secretariasenado.gov.co/senado/basedoc/ley/2004/ley_09060_204a.html [En línea].

[17] http://fgn.fiscalia.gov.co/Fiscalia/contenido/html/res02869_2003 [En línea].

[18] http://fgn.fiscalia.gov.co/Fiscalia/contenido/html/res06394_2004 [En línea].

[19] Torres. Daniel A. Cano, Jeimy J. Rueda, Sandra J. La evidencia digital en el contexto colombiano, Consideraciones técnicas y jurídicas para su manejo. [En línea]. Disponible: http://waww.acis.org.co/index.php?id=856.

[20] Cano M, Jeimy J**.** (2008). Introduccion a la informatica forense - "Una disciplina técnico – legal". [En línea]. Disponible: http://es.scribd.com/doc/34664173/Introduccion-Informatica-Forence-jEIMY-cANO-Phd-ACIS

[21] WILSON 2003, Taylor, R., Caeti, T., Kall Loper, D., Fritsch, E y Liederbach, J. 2006.

[22] Admin. (2005). Procedimiento Digital Forense. [En línea] Disponible: http://cibercrimen.blogspot.com/2005/10/e-procedimiento-forense-digital.html

[23] LOPEZ, Oscar., AMAYA, Haver., LEON, Ricardo**.** (2008). Informática forense - "Generalidades, aspectos técnicos y herramientas". [En línea]. Disponible: http://gluc.unicauca.edu.co/wiki/images/1/1d/InfoForense.pdf

BIBLIOGRAFIA

Ley 1273 del Enero 5 de 2009 - De la protección de la información y de los datos.

Ley 599 del 24 de Julio de 2000 – Código Penal

Ley 1032 de 2006 – Modificación al Código Penal

Ley 1266 del 31 de diciembre de 2008 - Hábeas Data

Ley 906 del 31 de Agosto de 2004 – Código de Procedimiento Penal "Sistema Acusatorio

Ley 527 de 1999 – El acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.

Resolución 0-2869 de diciembre 29 de 2003, de la Fiscalía General de la Nación - Manual de procedimientos de Cadena de Custodia.

Resolución 0-6394 de diciembre 22 de 2004, de la Fiscalía General de la Nación - Manual de procedimientos de Cadena de Custodia para el sistema penal acusatorio.

CANO M, Jeimy J. Computación Forense – "Descubriendo los rastros informáticos". Edición Alfaomega 2009.

SAPAG, Nasir. SAPAG, Reinaldo. Preparación y evaluación de proyectos. Edición McGraw-Hill 1995.

TAMAYO Y TAMAYO, Mario. Serie Aprender a Investigar, Módulo 5: El proyecto de investigación. 3ª Ed. Bogotá, ICFES, 1999. 237 p.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN, Trabajos Escritos: presentación y referencias bibliográficas (NTC 1486). Bogotá, ICONTEC, última actualización, julio de 2008.