MANEJO DE EVIDENCIA DIGITAL EN DISPOSITIVOS DE ALMACENAMIENTO PENDRIVE USB APLICANDO LA NORMA ISO/IEC 27037:2012

ING. JOSE BERNARDO CORTÉS DE LA ROSA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFÓRMATICA
PASTO
2014

MANEJO DE EVIDENCIA DIGITAL EN DISPOSITIVOS DE ALMACENAMIENTO PENDRIVE USB APLICANDO LA NORMA ISO/IEC 27037:2012

ING. JOSE BERNARDO CORTÉS DE LA ROSA

MONOGRAFÍA

Asesor
ING. ESP. HAROLD CABRERA MEZA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFÓRMATICA
PASTO
2014

Profundos agradecimientos a Dios, familiares, asesor, Universidad Nacional Abierta y a Distancia, que me apoyaron constantemente para el alcance de nueva esta meta.

CONTENIDO

pág.

LISTA DE FIGURAS

pag.

INTRODUCCIÓN

Durante el transcurso del presente trabajo, se centrará la atención en la evidencia digital contenida en dispositivos de almacenamiento pendrive USB comúnmente conocidos como memorias USB o memorias flash USB y sobre la norma ISO/IEC 27037:2012 que es reconocida como una directriz que brinda pautas comprobadas para la identificación, recolección y preservación de evidencia digital.

Un pendrive USB es un dispositivo flash pequeño y portátil que permite almacenar gran cantidad de datos entre los cuales puede existir información pertinente para un caso de informática forense, la cual al manejarse de una manera apropiada, se convertiría en evidencia digital de utilidad para la resolución de un caso expuesto ante un tribunal.

Durante el transcurso del presente trabajo, se realizará una introducción sobre los dispositivos de almacenamiento pendrive USB, posteriormente se presentarán lineamientos sobre la norma ISO/IEC 27037:2012 de evidencia digital, para finalmente explicar dichos lineamientos de tal manera que el lector pueda observar la aplicabilidad de la norma hacia el manejo de evidencia digital contenida en dispositivos de almacenamiento pendrive USB.

1. PROBLEMA DE INVESTIGACIÓN

1.1 DESCRIPCIÓN DEL PROBLEMA

En el campo de informática forense, existen algunas normas para el manejo de evidencia digital las cuales contienen pautas sobre procedimientos que se deben tener en cuenta durante la identificación, recolección y preservación de la evidencia.

Las normas existentes generalizan los procedimientos para los diferentes tipos de dispositivos que puedan contener evidencia de naturaleza digital. Al aplicar en dispositivos de almacenamiento USB como los pendrive dichos procedimientos, no se tendría la certeza de aplicar el procedimiento adecuado al dispositivo ya que la técnica podría ser la indicada para otro tipo de dispositivo pero no para un pendrive, generando como consecuencia que la calidad de la evidencia recolectada en estos dispositivos no sea la ideal y podría no haber sido recolectada en su totalidad, ser modificada accidentalmente, afectada durante su transporte y almacenamiento, perdiendo su credibilidad y valor al ser presentada ante un tribunal.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo asegurar la evidencia digital contenida en dispositivos de almacenamiento USB?

2 JUSTIFICACIÓN

El manejo adecuado de la evidencia digital es un proceso que se debe llevar de manera meticulosa por lo delicada y volátil que puede ser, por ello, al establecer de manera clara un procedimiento que permita manipular evidencia en dispositivos del tipo pendrive (memorias flash) dará un referente para los investigadores digitales sobre el cuidado que se debe seguir para la identificación, recolección y preservación de este tipo de dispositivos.

Al aplicar de manera eficiente los procedimientos de la norma ISO 27037:2012 para el manejo de evidencia digital en dispositivos de almacenamiento pendrive USB, se avala un recurso teórico que facilitaría a los peritos informáticos el manejo adecuado de las memorias flash para la identificación, recolección y preservación adecuada de estos dispositivos según las directrices que nos brinda la norma.

La aplicación adecuada de procedimientos para el manejo de evidencia digital en dispositivos pendrive va a contribuir en la calidad del material probatorio extraído de estos dispositivos, influenciando de manera directa en su aceptación ante el tribunal al cual se entregue.

De alcanzarse los objetivos planteados, el trabajo realizado va a servir como documento de consulta y ofreciendo algunas pautas de orientación ante futuras investigaciones concernientes a la temática de evidencia digital contenida en dispositivos USB de almacenamiento de datos y servirá como referente para el manejo de la norma ISO 27037 en el manejo de los dispositivos pendrive.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

- Aplicar la norma ISO/IEC27037:2012 en el manejo de evidencia digital contenida en dispositivos de almacenamiento pendrive USB.

3.2 OBJETIVOS ESPECÍFICOS

- Plantear procedimientos aplicables a la Norma ISO 27037:2012 para el manejo de evidencia digital contenida en dispositivos de almacenamiento pendrive USB.

- Explicar los lineamientos de la norma ISO/IEC:2012 que puedan ser enfocados hacia el manejo de evidencia digital contenida en un dispositivo de almacenamiento pendrive USB.

- Identificar normatividad colombiana para el manejo de evidencia digital presente en dispositivos de almacenamiento pendrive USB, aplicable a la norma ISO/IEC:2012.

4 MARCO REFERENCIAL

4.1 ANTECEDENTES

- Análisis Jurídico y Material de la Evidencia Digital en los Delitos Informáticos Judicializados por la Fiscalía en el Municipio de Bucaramanga en el Periodo 2006-2010. Tesis presentada por: Paula Andrea Álvarez David. Universidad Pontificia Bolivariana, Escuela de Derecho y Ciencias Políticas Tesis. Bucaramanga, Diciembre, 2011. La tesis busca una conceptualización de los delitos informáticos, sus objetivos, importancia, principios, el manejo material y jurídico de la evidencia digital dentro de una cadena de custodia, describiendo los pasos a seguir dentro de cada etapa durante el proceso de cadena de custodia.

  La tesis mencionada aporta al presente trabajo conocimiento delitos relacionados con las tecnologías y sobre algunos procedimientos sobre el manejo de dispositivos informáticos que contengan evidencia digital[1].

- Atipicidad Relativa en los Delitos de Falsedad, Hurto, Estafa y Daños Informáticos. Tesis de Grado presentada por: María Clara Fernández de Soto. Universidad Sergio Arboleda, Escuela de Derecho - Santa Marta 2001. El proyecto trata sobre modificaciones y en otros casos nuevas normas para disminuir en cierta forma la incertidumbre jurídica en que se encuentran sumergidas las nuevas disposiciones penales en materia de delito informático, pese a algunos avances, como la tipificación del acceso abusivo a sistemas informáticos. Contiene información muy interesante sobre la normatividad colombiana.

- Diseño de un Área Informática Forense para un Equipo de Respuestas Ante Incidentes de Seguridad Informáticos CSIRT. Tesis presentada por: la Ingeniera Mónica Alexandra Uyana García, República del Ecuador, Universidad de las fuerzas armadas ESPE, Enero del 2014. En este proyecto se propone el diseño de un área informática forense para un equipo especializado en el análisis y respuestas ante Incidentes de

[1] ÁLVAREZ DAVID, Paula Andrea. Análisis Jurídico y Material de la Evidencia Digital en los Delitos Informáticos Judicializados por la Fiscalía General de la Nación en el Municipio de Bucaramanga en el Periodo 2006-2010. Tesis. Bucaramanga: Universidad Pontificia Bolivariana, Escuela de Derecho y Ciencias Políticas, Diciembre, 2011. p. 12-16, 68-76, 80. Consultado en: http://repository.upb.edu.co:8080/jspui/bitstream/123456789/1834/1/digital_22203.pdfp.

Seguridad Informáticos (CSIRT) en el Ecuador, basada en las mejores prácticas y directrices que permitan realizar la recopilación, preservación, análisis, procesamiento, reportes y almacenamiento de pruebas y evidencias digitales.

Aporta al presente trabajo información sobre la clasificación de la evidencia digital e información sobre diferentes guías para la recolección de evidencia digital[2].

- Metodología Para la Implementación de Informática Forense en Sistemas Operativos Windows y Linux. Proyecto de grado presentado por el ingeniero Omar Ramiro Almeida Romo. En la ciudad de Ibarra, Ecuador, Universidad Técnica del Norte, Facultad de Ingeniería en Ciencia Aplicadas.

  Por medio de su proyecto, el autor pretende aportar un estudio general acerca de la disciplina de la informática forense, planteando una metodología que permita una búsqueda estructurada de indicios que ayuden en investigaciones de hechos punibles.

  Aporta información sobre las fases tenidas en Cuenta en el Ecuador para la investigación la que intervenga evidencia digital[3].

- Manual Básico de Cateo y Aseguramiento de Evidencia Digital[4], Del autor Gabriel Andres Campoli. Se trata de un manual que tiene por objeto servir como una guía de las acciones y mecanismos mínimos a aplicar para el cateo o aseguramiento de los equipos electrónicos hallados en la escena de un crimen y que pudieran contener evidencia digital.

---

[2] UYANA GARCÍA, Mónica Alexandra, Ing. Diseño de un Área Informática Forense para un Equipo de Respuestas Ante Incidentes de Seguridad Informáticos CSIRT. Tesis de grado. Sangolquí: Universidad de las Fuerzas Armadas ESPE del Ecuador. 2014. p. 60-79, 233

[3] ALMEIDA ROMO, Omar Ramiro. Metodología para la implementación de informática forense en sistemas operativos Windows y Linux. Trabajo de Grado. Ibarra: Universidad Técnica del Norte. Facultad de Ingeniería en Ciencia Aplicadas, 2011. p. 124-143. Consultado En: http://repositorio.utn.edu.ec/bitstream/123456789/539/7/04%20ISC%20157%20CAPITULO%20II.pdf

[4] CAMPOLI, Gabriel. Manual Básico de Cateo y Aseguramiento de Evidencia Digital. En: Revista de Derecho Informático. 2006, no 99. p. 3-8.

Este trabajo aporta a la presente monografía detalles a tener en cuenta para evitar sufrir las consecuencias de la nulidad de las pruebas al ser presentadas frente a un tribunal.

4.2 MARCO CONCEPTUAL

- Bloqueadores de escritura. Son equipos que evitan la escritura en los dispositivos a los cuales se conectan permitiendo de esta manera evitar cambios y modificaciones en dichos dispositivos.

- Bolsas Faraday. Son bolsas especialmente diseñadas para la recolección, preservación, transporte y análisis de dispositivos móviles e inalámbricos.

  El material de estas bolsas forman un blindaje alrededor de teléfonos celulares, GPS, netbooks, dispositivos bluetooth, laptops, etc., bloqueando toda señal celular, WIFI o de radio.

  Una vez dentro de la bolsa de faraday, el dispositivo no podrá volver a conectarse con la red aunque se encuentre encendido, asegurando que el mismo no pueda ser controlado, localizado o bloqueado remotamente[5].

- Cadena de Custodia. Conjunto de procedimientos que permitirán alcanzar niveles de efectividad para asegurar las características originales de los elementos materia de prueba o evidencias físicas desde su recolección hasta su disposición final, dentro de una dinámica constante de mejoramiento y modernización, con el fin único de satisfacer las necesidades y expectativas de la administración de justicia para lograr una pronta y cumplida justicia[6].

[5] DIVISIÓN FORENSE. Productos e Insumos de Criminalística. Bolsa de Faraday Para Dispositivos Móviles. Buenos Aires: División Forense, 2014. Disponible en Internet: https://www.division-forense.com/bolsa-faraday.html

[6] REPÚBLICA DE COLOMBIA. FISCALÍA GENERAL DE LA NACIÓN. Manual de Procedimientos Para Cadena de Custodia. Op. cit., p. 9.

- Cifrado. “Proceso de aleatorización o codificación de datos para que sólo los usuarios previstos pueden tener acceso a ellos”[7].

- Delito Informático. No existe una definición universal para delito informático, pero la siguiente definición se aproxima en gran medida. Se define como cualquier conducta criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que en sentido estricto el delito informático es cualquier acto ilícito penal en el que los equipos de cómputo, sus técnicas y funciones desempeñan un papel ya sea con el método, medio o fin[8].

- Embalaje. “Es la maniobra que se realiza para guardar, inmovilizar y proteger un indicio, dentro de algún recipiente protector (sobres, envases, frascos, entre otros)”[9].

- Etiquetado. Es la rotulación adecuada con todos los datos necesarios que identifican y describen lo más precisamente posible la evidencia, mencionando marcas, colores y detalles propios de la misma; especificando el lugar en donde se recolectaron, dirección de la inspección, hora y fecha, así como nombre y firma de quien la recolectó. Para esto se pueden hacer uso de etiquetas diseñadas para tal fin o escribir con el respectivo cuidado en el recipiente o bolsa que sirve de embalaje, actividad que debe realizarse antes de introducir la evidencia.

- Evidencia Digital. “Abarca cualquier información en formato digital que pueda establecer una relación entre un delito y su autor. Desde el punto de vista del derecho probatorio, puede ser comparable con un documento como prueba legal”[10].

---

[7] ESTADOS UNIDOS DE AMÉRICA. FEDERAL BUREAU OF INVESTIGATION, FBI. Digital Evidence field Guide: What Every Peace Officer Must Know. Op. cit., p. 22.

[8] LIMA MALVIDO, María de la Luz. Delitos electrónicos. Ciudad de México: Academia Mexicana de Ciencias Penales, 1984. p. 100.

[9] GRUPO IBEROAMERICANO DE TRABAJO EN LA ESCENA DEL CRIMEN, GITEC. Manual de Buenas Prácticas en la Escena del Crimen, AICEF/GITEC. 1 ed. México, D.F.: Instituto Nacional de Ciencias Penales, 2010. p. 70.

[10] TORRES, Daniel; CANO, Jeimy; RUEDA, Sandra. Evidencia Digital en el Contexto Colombiano: Consideraciones Técnicas y Jurídicas Para su Manejo. ACIS. 2006. Disponible en Internet: http://www.acis.org.co/index.php?id=856.

- Función Hash. Se define como una operación que se realiza sobre un conjunto de datos de cualquier tamaño de tal forma que se obtiene como resultado, otro conjunto de datos denominado “resumen”, el cual tiene un tamaño fijo e independiente del tamaño original, que además tiene la propiedad de estar asociado unívocamente a los datos iniciales[11].

- Información Digital. “Se trata de información que es almacenada electrónicamente desglosada en dígitos o unidades binarias de unos y ceros que se guardan y se recuperan mediante un conjunto de instrucciones llamados programas o código”[12].

- Informática Forense. “La Informática forense es una disciplina dedicada a la recolección de pruebas digitales desde una maquina computacional para fines judiciales mediante la aplicación de técnicas de análisis y de investigación”[13].

- Medios extraíbles. Son dispositivos que almacenan datos que pueden ser fácilmente removidos y ocultados, como disquetes, CD, DVD, tarjetas de memoria flash, y dispositivos pendrive USB [14] .

- Medio Informático. Cualquier dispositivo electrónico capaz de manejar información digital.

- Norma ISO/IEC 27037. Es una directriz que proporciona pautas en actividades específicas como identificación, recolección y preservación de potencial evidencia digital que pueda tener un valor probatorio[15].

---

[11] TAMAYO, PABLO. Tutorial, citado por Lituma, Marco. Criptografía: Funciones Hash como alternativa de seguridad en Transacciones Online para Organizaciones o Empresas. Sf. p. 25-26.

[12] ESTADOS UNIDOS. NATIONAL FORENSIC SCIENCE TECHNOLOGY CENTER, NFSTC. A Simplified Guide to Digital Evidence. Florida: El Centro, 2012. p. 3.

[13] CABRERA MESA, Harold Emilio, ing. esp.. Informática Forense, Unidad 1. Fundamentos de la Informática Forense. Pasto: Universidad Nacional Abierta y a Distancia, UNAD, 2013. p. 3. Disponible en Internet: http://datateca.unad.edu.co/contenidos/233012/unidad_1/u1_introduccion%20a%20la%20informatica%20forense.pdf

[14] --------. FEDERAL BUREAU OF INVESTIGATION, FBI. Digital Evidence field Guide: What Every Peace Officer Must Know. Op. cit., p. 22.

[15] Organización Internacional de Normalización, ISO. Standards Catalogue ISO/IEC 27037:2012. Genova: La ISO, 2012. Disponible en Internet: www.iso.org/iso/catalogue_detail?csnumber=44381

- Sanitizar. Término utilizado por INTECO para hacer referencia a un borrado seguro de dispositivos magnéticos en función de la confidencialidad de la información que contiene.

- UTC. Son las siglas internacionales para Tiempo Universal Coordinado. Es el estándar de hora universal basado en el empleo de relojes atómicos de gran precisión.

4.3 MARCO LEGAL

El Gobierno de Colombia en los últimos años ha realizado un considerable esfuerzo en el desarrollo normativo sobre el manejo de evidencia digital y su estadía dentro de una cadena de custodia, promoviendo una legislación que dé cumplimiento a los derechos de los ciudadanos y entes organizacionales, permitiendo que las instituciones cuenten con herramientas necesarias para enfrentar, investigar, procesar, judicializar y penalizar conductas delictivas en las cuales intervengan medios informáticos.

Entre la normatividad existente se destaca:

- Ley 489. (29, Diciembre, 1998). Por la cual se dictan normas sobre la organización y funcionamiento de las entidades de orden nacional

- Ley 599. (24, Julio, 2000). Sobre la violación a la intimidad, reserva e interceptación de comunicaciones.

- Ley 600 de 2000. (24, Julio, 2000). Toda investigación debe fundarse en pruebas legales oportunamente vinculadas a la actuación.

- Ley 678. (3, Agosto, 2001). Por medio de la cual se expide un estatuto para prevenir y contrarrestar la pornografía infantil.

- Ley 906. (1, Enero, 2005). Fiscalía tiene la atribución para ordenar registros, allanamientos, incautaciones e interceptaciones de comunicaciones.

- Ley 1273. (5, Enero, 2009). Por la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos”.

- Ley 1336. (21 Julio, 2009). Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía infantil.

- Sentencia C-662/00. (8, Junio, 2000). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos.

- Resolución 000435. 1 EF. (1, Enero, 2005). Por la cual se hace entrega del “Manual de Procedimientos Bodega de Evidencias “.

- Resolución 0-1890. (5, Noviembre, 2002). Por medio de la cual reglamenta el artículo 288 de la ley 600.

- Resolución 0-2869. (29, Diciembre, 2003). Por medio de la cual se adopta el Manual de Procedimientos del Sistema de Cadena de Custodia.

- Resolución 0-6394. (22, Diciembre, 2004). Por medio de la cual se adopta el manual de procedimientos del Sistema de Cadena de Custodia para el Sistema Penal Acusatorio

- Acuerdo PSAA06-3334. (2, Marzo, 2006). Por el cual se reglamentan la utilización de medios electrónicos e informáticos en el cumplimiento de las funciones de administración de justicia.

- Decreto 1360. (23, Junio, 1989). Por el cual se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor.

- Decreto 1747. (11, Septiembre, 2000). Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación.

4.4 MARCO TEÓRICO

4.4.1 Historia de los Dispositivos de Almacenamiento Pendrive

Desde su nacimiento a mediados de los 90, los interconectores de conexión USB (Universal Serial Bus) se han convertido en uno de las tecnologías más utilizadas a nivel mundial, llegando a desplazar a sus antecesores que poco a poco van quedando en el olvido.

Posiblemente entre los principales elementos que permitieron un acogimiento masivo de esta tecnología, fue el contar con un conector estándar, la no utilización de cables y conectores específicos para cada dispositivo, su compatibilidad con múltiples plataformas y sistemas operativos, adicionalmente su estandarización que permite la conexión de múltiples clases de dispositivos electrónicos utilizados hoy en día y esto sin mencionar que la mayoría de los dispositivos USB no necesitan conectarse a una fuente externa de energía debido a su capacidad de alimentación desde el mismo puerto conector.

Un pendrive es un dispositivo electrónico de almacenamiento no volátil pensado para ser utilizado como disco duro externo portátil. Utiliza memoria de tipo flash la cual le permite conservar la información almacenada sin necesidad de una fuente continua de energía[16].

Los dispositivos pendrive de almacenamiento USB son un medio muy difundido en la actualidad, entre las ventajas que poseen este tipo de dispositivos se encuentra su bajo costo, tamaño reducido, alta capacidad y confiabilidad en el almacenamiento de datos, facilidad de transporte, teóricamente pueden retener los datos almacenados durante 20 años, reescribirse un millón de veces, permite procesos simultáneos de lectura/escritura, su diseño de estado sólido las protege de abusos ocasionales, al no tener partes movibles su periodo de duración es mayor y adicionalmente las demás ventajas nombradas anteriormente de los interconectores USB.

La memoria flash de un dispositivo de almacenamiento pendrive posee una amplia ventaja frente a su antecesora EEPROM (Electrical Erasable PROM), la memoria flash puede ser borrada y reprogramada al conectarse a un equipo de cómputo y además permite el borrado bloque a bloque, mientras que una

[16] GOBIERNO DE ESPAÑA. MINISTERIO DE ECUACIÓN, CULTURA Y DEPORTE. Usos Avanzados de una Memoria USB. Disponible en Internet: http://recursostic.educacion.es/observatorio/web/eu/equipamiento-tecnologico/hardware/703-usos-avanzados-de-una-memoria-usb

memoria EEPROM necesita de un dispositivo especial llamado lector de PROM. Esta es una característica que facilita su utilización pero que a la vez implica tener un mayor cuidado con la información almacenada en el dispositivo en el momento de borrar archivos.

Las primeras unidades de almacenamiento pendrive USB fueron creadas por IBM (International Business Machines Corp), quienes en su afán por encontrar un reemplazo de las unidades de disquete para su línea de productos ThinkPad, desarrollaron esta tecnología de la mano con M-Systems.

Los primeros pendrive fabricados poseían capacidades de almacenamiento de 8, 16, 32 y 64 Mb, lo cual superaba en gran medida a sus antecesores los disquetes de 5 ¼ y de 3 ½ que en el mejor de los casos almacenaban un máximo de 1,4 Mb. En la actualidad, la capacidad ha aumentado considerablemente, encontrando en el mercado dispositivos de almacenamiento pendrive USB de hasta 1Tb como es el caso de la memoria Hipex Predator 3.0 lanzada al mercado el presente año por Kingston.

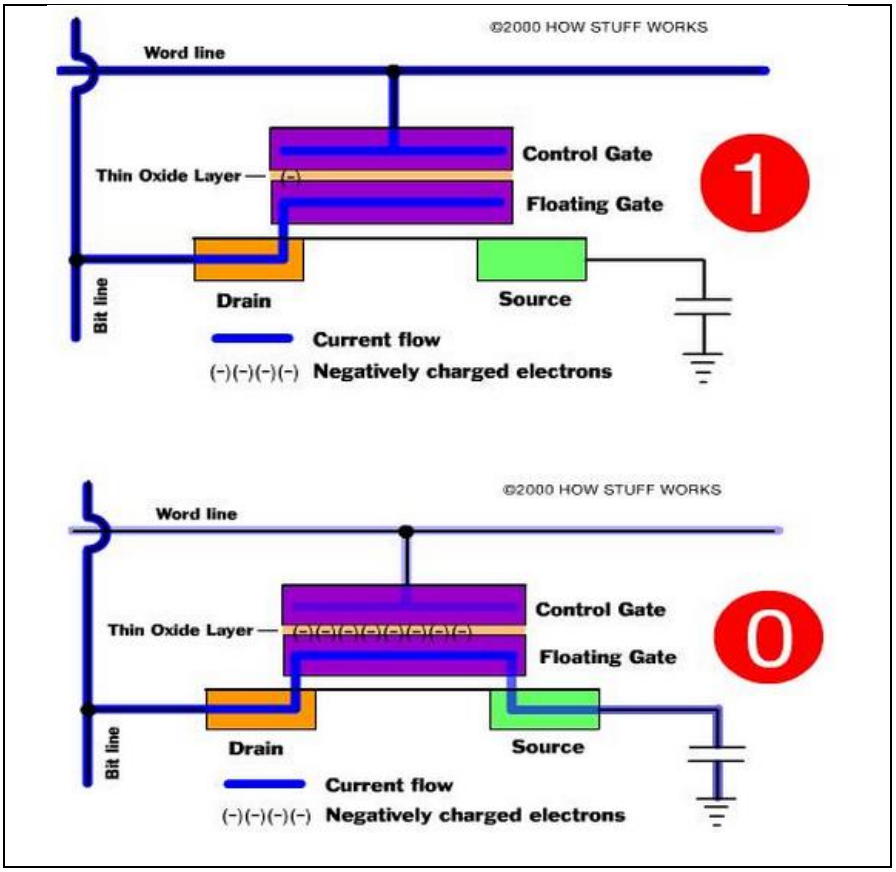
4.4.2 Funcionamiento de un PenDrive

Las memorias flash que poseen internamente los pendrive se componen de dos transistores separados entre sí por una fina capa de óxido. Uno de los transistores se llama “puerta flotante” y es el que almacena los electrones, el otro se denomina “puerta de control” el cual es el encargado de generar el campo eléctrico. La presencia o no de corriente se detecta e interpreta como un 1 o un 0 reproduciendo el dato almacenado[17].

La mayoría de estos dispositivos de almacenamiento utilizan como formato el sistema de archivos FAT32 debido a la simplicidad de este sistema que facilita la comunicación mediante un puerto USB, sin embargo el usuario final tiene la opción de formatear el dispositivo bajo el sistema de archivos de su preferencia según las posibilidades permitidas por su sistema operativo.

[17] CENTRO INTERACTIVO DE CIENCIA Y TECNOLOGÍA HORNO3. Divulgación de la Ciencia. Boletín 58. Monterrey: 2013. Disponible en Internet: horno3.ensi.com.mx/apps/newsletter/idem.php?module=Newsletter&action=ReadNewsletter&newsletter_id=4782

Figura 1. Funcionamiento de un PenDrive



Fuente: Centro Interactivo de Ciencia y Tecnología Horno3. Divulgación de la Ciencia.

4.4.3 Clasificación de un Pendrive Según la Velocidad de Transmisión de Información

Según la velocidad en la transmisión de los datos, los dispositivos de almacenamiento pendrive USB se clasifican en:

- USB 1.0 de velocidad hasta 1,5 Mbps
- USB 1.1 de velocidad hasta 12 Mbps
- USB 2.0 de velocidad hasta 480 Mbps
- USB 3.0 de velocidad hasta 4.8 Gbps

4.4.4 Sobre la Evidencia Digital

Según Ghosh, la Evidencia Digital se define como "Cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático" [18]. 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.

El FBI define a la Evidencia Digital como datos que han sido procesados electrónicamente y almacenados o transmitidos a través de un medio informático.

Según Casey, la evidencia digital es un tipo de evidencia física construida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales[19].

4.5 FUNCIONES HASH CRIPTOGRÁFICAS

Las funciones hash criptográficas convierten un mensaje de cualquier tamaño en un mensaje de una longitud constante, son utilizadas en procesos de autenticación, o de comprobación de integridad de datos.

Al aplicar una función hash criptográfica a un mensaje se obtiene un resumen criptográfico o huella digital. Es decir, a partir de un número indeterminado de bits, siempre se obtiene un número constante y diferente que identifica de forma unívoca a ese flujo de datos[20].

---

[18] GHOSH, Ajoy. Incident Response and Forensics Workshop. Doc No: telwg29/IRF/04a, Australia: Guidelines for the Management of IT Evidence, 2004. p. 9. Disponible en Internet: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf

[19] CASEY, E. Digital Evidence and Computer Crime. Citado por CANO, Jeimy. Admisibilidad de la Evidencia Digital: De los conceptos legales a las Características Técnicas. Trabajo de grado. Bogotá D.C.: Universidad de Los Andes. Facultad de Derecho, 2003. p.2. Disponible en Internet: file:///C:/Users/Jose/Downloads/EJUS_BOGOTA_2007_EVIDENCIA_DIGITAL_EN_COLOMBIA.pdf

[20] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Cómo Comprobar la Integridad de los Ficheros. INTECO: Madrid, s.f. p. 2.

4.5.1 Características de las Funciones Hash

Según el Instituto Nacional de Tecnologías de la Comunicación de España INTECO[21], las funciones Hash deben ser públicas y de código abierto, la función no puede ser invertible, es decir que no se puede encontrar una función o un algoritmo que sea capaz de computar el mensaje original a partir del resumen criptográfico, no debe ser posible generar un mensaje con un resumen criptográfico determinado a no ser que se utilice un método de fuerza bruta, es decir, probando con mensajes arbitrarios hasta obtener el resumen criptográfico deseado, no debe existir un método, si se cambia un bit del mensaje, tiene que cambiar el resumen criptográfico en por lo menos un 50%, siempre que se aplique la función a un mensaje, se debe obtener el mismo resultado.

[21] Ibid., p. 3.

4.6 NORMA ISO/IEC 27037:2012

La norma ISO/IEC 27037 se publicó en el 2012, bajo el nombre de “Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence”.

ISO 27037 Es una directriz que proporciona pautas en actividades específicas como identificación, recopilación, consolidación y preservación de potencial evidencia digital que pueda tener un valor probatorio[22].

Si la recolección de evidencia se hace correctamente, es mucho más útil y va a permitir aprender sobre el atacante, por otra parte, bajo estas condiciones la evidencia va a tener una mayor probabilidad de ser admisible dentro de un proceso judicial.

4.6.1 Orientación Para Dispositivos

La norma ISO / IEC 27037:2012 proporciona orientación para los siguientes dispositivos y circunstancias [23] . Se nombra una lista indicativa más no exhaustiva:

- Medios de almacenamiento digital utilizados en ordenadores estándar como discos duros, disquetes, ópticos y discos magneto-ópticos, dispositivos de datos con funciones similares.
- Teléfonos móviles, asistentes personales digitales (PDA), dispositivos electrónicos personales (PED), tarjetas de memoria.
- Sistemas de navegación móviles.
- Cámaras digitales de vídeo (incluyendo CCTV).
- Equipo estándar con conexiones de red.
- Redes basadas en TCP / IP y otros protocolos digitales.
- Dispositivos con funciones similares a las anteriores.

[22] Organización Internacional de Normalización, ISO. Standards Catalogue ISO/IEC 27037:2012. Op.cit. Disponible en Internet: www.iso.org/iso/catalogue_detail?csnumber=44381

[23] Ibid.

4.6.2 Principios Básicos de la Norma ISO/IEC 27037 Durante Recolección de Evidencia

- Es necesario adherirse a las políticas y normas de su país. Adicionalmente, asignar el manejo de Incidentes en los cuales se involucre evidencia digital a instituciones y servidores avalados por las leyes de su país.

- Cualquier servidor designado para el manejo de la diligencia no deberá tomar acciones más allá de sus competencias

- Capturar de una imagen del dispositivo lo más exacta que sea posible y tan pronto como el dispositivo se encuentre a disposición del experto.

- Mantener documentación detallada de cada procedimiento realizado, incluyendo siempre fecha y hora de cada acción. Si es posible se debe generar una transcripción digital de los informes. Tener en cuenta que para esta labor no se deberá utilizar ningún dispositivo o medio de comunicación que haga parte del material a investigar. Cada nota e impresión deberá estar firmada y fechada.

- Tener en cuenta la diferencia entre el reloj del sistema y la hora UTC. para cada marca de tiempo, registrar los dos registros de hora.

- Esté preparado para testificar (quizás esto ocurra años más tarde), por esto se debe registrar y conservar lo registros detallados de todas acciones que se efectuaron en aquel momento. Las notas detalladas serán vital ayuda para estos casos.

- Evitar al máximo realizar cambios en la información digital que se esté recopilando, tanto en su contenido, como en el registro de los tiempos de acceso del directorio. Evitar que se produzcan actualizaciones en los archivos.

- Desconectar posibles medios de comunicación del dispositivo.

- Cuando se enfrente ante una elección entre la recolección y el análisis, primero se procederá a la recolección y posteriormente a un análisis.

- Los procedimientos que se efectúen deben ser puestos a prueba con anterioridad para asegurar su viabilidad ante una crisis. Si es posible, los

procedimientos deben ser automatizados por razones de velocidad y precisión. Sea metódico.

- Se debe adoptar un procedimiento metódico para cada dispositivo, siguiendo las directrices establecidas en el procedimiento de recaudación de la evidencia.

- Proceda a recoger evidencia teniendo en cuenta el nivel de volatilidad de la misma, se debe iniciar de la más a la menos volátil.

- Se debe realizar una imagen a nivel de bit de los medios originales. El análisis forense de búsqueda se deberá realizar utilizando la imagen. ya que este va a variar los horarios de acceso a archivos.

4.6.3 Orden Recolección de Evidencia Según la Volatilidad

Para la recolección de evidencia se debe proceder teniendo en cuenta el nivel de volatilidad comenzando por la más a la menos volátil.

- Registros, caché

- Estadísticas de la tabla de enrutamiento, caché arp, la tabla de procesos, kernel, memoria.

- Sistemas de archivos temporales

- Disco

- El registro remoto y los datos de seguimiento relevantes para la sistema en cuestión

- Configuración física, la topología de red

- Soporte de archivo

4.6.4 Situaciones que Evitar

Es muy fácil de destruir pruebas, aunque inadvertidamente, por esto se lista una serie de acciones que se deben evitar para evitar la pérdida de evidencia digital.

- No apague ningún dispositivo hasta estar seguro de haber completado la recopilación de evidencia. Hay mucha evidencia que se puede perder posiblemente el atacante pudo haber alterado el equipo para que las evidencias se destruyan una vez el equipo sea apagado.

- No ejecute programas que modifican el tiempo de acceso de todos los archivos en el sistema (por ejemplo, 'tar' o 'xcopy').

4.6.5 Consideraciones de Privacidad

- Respetar las normas y directrices de la empresa en cuanto a su privacidad según la normatividad legal. En particular, se debe asegurar de que la información recogida junto con la evidencia que está buscando no se encuentre por ningún motivo disponible para personas que normalmente no tendrían acceso dicha información. Esto incluye el acceso a los archivos de registro (que pueden revelar patrones de comportamiento de los usuarios), así como los datos y archivos personales.

- No inmiscuirse en la vida privada de las personas si no se tiene una justificación. No recoger información de áreas en las que normalmente no tienen razones para el acceso (por ejemplo, almacenes de archivos personales) a menos que se tengan sospechas justificadas de la presencia de material probatorio.

- Se debe estar seguro de tener el respaldo de la empresa para realizar los procedimientos y medidas que permitan recopilar evidencia de un incidente.

4.6.6 Consideraciones Legales

Según la norma ISO 27037, la evidencia digital tiene que ser:

- Ser Admisible. La evidencia Digital debe ajustarse a ciertas normas legales antes de que pueda ser puesta ante un tribunal.
- Ser Auténtica. La evidencia Digital debe permitir vincular el material probatorio con el incidente.
- Estar Completa. Debe contar toda la historia y no sólo una perspectiva particular.
- Ser Confiable. No debe generar duda alguna sobre la autenticidad, veracidad y la transparencia de la evidencia desde su recolección, manejo durante el proceso de cadena de custodia, hasta su entrega final ante un tribunal.
- Ser Creíble. Debe ser fácilmente creíble y comprensible por un tribunal.

4.6.7 Procedimiento de Aseguramiento

La evidencia debe ser estrictamente asegurada. Además, la cadena de custodia debe estar claramente documentada.

Cadena de Custodia

Debe documentarse:

- Dónde, cuándo y por quién fue descubierta y recogida la evidencia.
- Dónde, cuándo y por quién manipuló o examinó la evidencia.
- Quién tenía la custodia de las evidencias y durante qué período.

- Cómo fue almacenada la evidencia.
- Cuando la evidencia cambió de custodia, cuándo y cómo se hizo la transferencia (incluyen los números de envío, etc).

Dónde y cómo Almacenar

De ser posible, los medios los medios físicos se deben almacenar en un lugar oscuro.

Acceso a las pruebas debe ser muy restringido, y debe ser claramente documentado.

Debería ser posible detectar el acceso no autorizado.

4.6.8 Herramientas Necesarias

Se debe tener los programas que necesarios para realizar la recopilación de pruebas en medios de sólo lectura, así como el conjunto de herramientas para cada uno de los sistemas operativos que a los cuales se vaya a tener acceso.

El conjunto de herramientas debe incluir:

- Un programa para el examen de los procesos (por ejemplo, 'ps').
- Programas para examinar el estado del sistema (por ejemplo, 'showrev', 'ifconfig', 'netstat', 'arp').
- Un programa para hacer copias bit a bit (por ejemplo, 'DD', 'SafeBack').
- Programas para generar sumas de comprobación y firmas (por ejemplo, 'sha1sum', un 'dd' checksum, 'SafeBack').

5 DISEÑO METODOLÓGICO PRELIMINAR

5.1 TIPO DE INVESTIGACIÓN

Investigación Exploratoria

La norma ISO/IEC27037:2012 es un referente de directrices sobre el manejo de evidencia digital. Adicionalmente se trata de una norma reciente publicada hace apenas dos años, por este motivo vale la pena proponer estudios que permitan de una u otra manera servir de referente para posteriores estudios, permitiendo obtener una visión aproximada de la realidad sobre la aplicabilidad de la norma hacia evidencia digital contenida en dispositivos de almacenamiento USB tipo pendrive.

5.2 METODOLOGÍA DE LA INVESTIGACIÓN

Existe un problema de incertidumbre en la aplicación de procedimientos adecuados para el manejo de evidencia digital contenida en dispositivos de almacenamiento USB de tipo pendrive. Se desea encontrar una solución al problema que se plantea, para lo cual inicia un proceso de recolección de información que permita llegar a una solución.

El proceso de recolección inicia con elementos que permitan realizar una breve contextualización sobre los dispositivos de almacenamiento USB tipo pendrive, teniendo en cuenta aspectos relevantes de la historia, funcionamiento y clasificación. La contextualización preliminar incluyó también información sobre las funciones hash al ser un tema de relevancia en el manejo de la norma ISO tratada.

Los esfuerzos comienzan a centrarse en encontrar una norma que reconocida y con respaldo que incluya lineamientos que permitan un adecuado manejo de la evidencia contenida en dispositivos USB tipo pendrive, la norma que se selecciona es la ISO/IEC 27.037:2012, la cual se especializa en el manejo de evidencia digital.

Una vez identificada la norma sobre la cual trabajar, se necesitaba averiguar si dicha norma además de ser apta para el manejo de evidencia digital, esta contenía procedimientos específicos para el manejo de evidencia digital contenida en dispositivos de almacenamiento tipo pendrive.

Para esto, se procede a buscar toda la información disponible sobre la norma, una vez terminado el proceso de recolección se la organiza se organiza la información y expone de tal manera que se pueda apreciar en rasgos generales el contenido y alcance de la norma.

Posteriormente se procede a analizar cada detalle de la norma y además, se recolecta información sobre diferentes tipos de procedimientos aplicables a la norma estudiada, con esto se logra identificar procedimientos que podrían aplicables a la norma ISO 27037

Con toda la información reunida y análisis previos se inicia un proceso de análisis final que va a permitir determinar una manera viable de asegurar la evidencia digital contenida en dispositivos de almacenamiento USB.

6 APLICACIÓN DE LA NORMA ISO/IEC 27037:2012 AL MANEJO DE UN DISPOSITIVO DE ALMACENAMIENTO PENDRIVE USB

6.1 DISPOSITIVOS QUE ORIENTA LA NORMA ISO/IEC 27037:2012

La norma hace mención sobre la orientación a medios de almacenamiento digital utilizados en ordenadores estándar como discos duros, disquetes, ópticos y discos magneto-ópticos, dispositivos de datos con funciones similares.

Los pendrive USB entran en este grupo al ser dispositivos de almacenamiento digital utilizados en ordenadores estándar y se incluyen dentro de la clasificación "dispositivos de datos con funciones similares".

Esto quiere decir que desde este momento es viable aplicar la norma a los dispositivos pendrive.

6.2 PRINCIPIOS BÁSICOS DE LA NORMA ISO/IEC 27037 DURANTE LA RECOLECCIÓN DE EVIDENCIA APLICADOS A PENDRIVES

6.2.1 Políticas de Cada País

La norma ISO plantea que es necesario acoplarse a las políticas y normas de cada país. Adicionalmente, asignar el manejo de Incidentes en los cuales se involucre evidencia digital a instituciones y servidores avalados por las leyes de su país.

En Colombia, instituciones como la Fiscalía, el CTI, la DIJIN, el Ejército y la Policía cuentan con personal capacitado para el manejo de evidencia digital.

Se retoma nuevamente la normatividad colombiana anteriormente descrita en el marco legal que de manera directa o indirecta pueda involucrar el manejo de evidencia digital contenida en un pendrive:

El Gobierno de Colombia en los últimos años ha realizado un considerable esfuerzo en el desarrollo normativo sobre el manejo de evidencia digital y su manejo dentro de una cadena de custodia, promoviendo una legislación que dé cumplimiento a los derechos de los ciudadanos y entes organizacionales, permitiendo que las instituciones cuenten con herramientas necesarias para

enfrentar, investigar, procesar, judicializar y penalizar conductas delictivas en las cuales intervengan medios informáticos.

Por medio de la resolución 1890 del Noviembre 5 de 2002, la Fiscalía General de la Nación[24], ordena la aplicación de un proceso para el manejo de los elementos materiales probatorios (EMP) y evidencias físicas (E.F), que contempla procedimientos con actividades que van desde el aseguramiento de la escena hasta la disposición final de los mismos.

En la Constitución de Colombia, el término EMP se generaliza para material probatorio no físico, dentro del cual se encuentra incluida la evidencia de naturaleza digital, por lo cual cada vez que se haga referencia a elemento material probatorio dentro de las leyes que se citan a continuación, se referencia de manera indirecta a la evidencia digital.

En Diciembre 29 de 2003, la Fiscalía[25] publica la resolución 0-2869, por medio de la cual la se estandarizan procedimientos en un primer manual para cadena de custodia, en el que se unifican rótulos, formatos y se ofrecen recomendaciones de prácticas para el debido manejo de la recolección, embalaje de indicios y la necesidad de adecuación de los almacenes de evidencia para la custodia de los EMP y EF.

Posteriormente en Diciembre de 2004, la Fiscalía General de la Nación[26] por medio de la resolución 0-6394, adopta el manual de procedimientos del sistema de cadena de custodia para el sistema penal acusatorio.

En Septiembre 11 de 2000, la Presidencia de la República da a conocer el Decreto 1747, por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales[27].

---

[24] REPÚBLICA DE COLOMBIA. FISCALÍA GENERAL DE LA NACIÓN. Resolución 0-2869. Op. cit.

[25] --------. Resolución 0-1890. (5, Noviembre, 2002). Por medio de la cual reglamenta el artículo 288 de la ley 600. Bogotá, D.C., 2002.

[26] --------. Resolución 0-6394. (22, Diciembre, 2004). Por medio de la cual se adopta el manual de procedimientos del Sistema de Cadena de Custodia para el Sistema Penal Acusatorio. Diario Oficial. Bogotá, D.C.: 2004. no 45772. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=15634

[27] --------. Decreto 1747. (11, Septiembre, 2000). Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales. Diario Oficial. Bogotá, D.C., 2000. no 44160. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4277

En el Decreto 1360 de 1989 entregado por el Ministerio de Gobierno y la Presidencia de la República, se reglamentan la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor.

Por medio del Acuerdo No. PSAA06-3334, de Marzo 6 de 2006, la Sala Administrativa del Consejo Superior de la Judicatura reglamenta la utilización de medios electrónicos e informáticos en el cumplimiento de las funciones de administración de justicia.

Adicionalmente, vale la pena resaltar la ley 600 del 24 de Julio del 2000, puesto que por medio de esta ley el Congreso de la República[28], expide en el Código de Procedimiento Penal que toda investigación debe fundarse en pruebas legales oportunamente vinculadas a la actuación, considerando como medios de prueba la inspección, la peritación, el documento, el testimonio, la confesión y el indicio y será deber del funcionario judicial tomar las medidas necesarias para evitar que los elementos materiales de prueba sean alterados, ocultados o destruidos.

Para la obtención de pruebas de hechos punibles la ley 600 opta por una inspección en el lugar de los hechos, donde cualquier resultado se registrará dentro de un acta que describa detalladamente las manifestaciones que hagan las personas que intervengan en la diligencia y los elementos probatorios útiles se conservarán y recogerán, teniendo en cuenta los procedimientos de cadena de custodia[29].

Si se requiere la práctica de pruebas técnico-científicas al material probatorio encontrado, el funcionario judicial podrá solicitar la presencia de un perito para este fin, quien examinará los elementos materia de prueba, dentro del contexto de cada caso y a su vez, será el perito quien exponga y explique los resultados obtenidos ante una audiencia, los procedimientos realizados y el total cumplimiento de una cadena de custodia en sus acciones[30].

La ley 600 menciona que se debe aplicar la cadena de custodia a los elementos físicos y EMP, para garantizar la autenticidad de los mismos,

---

[28] REPÚBLICA DE COLOMBIA. CONGRESO DE LA REPÚBLICA. --------. Ley 600 de 2000. (24, Julio, 2000). Por la cual se expide el Código de Procedimiento Penal. Diario Oficial. Bogotá, D.C., 2000. no 44097. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6389

[29] Ibid., Capítulo II, Artículo 244.

[30] Ibid., Capítulo II, Artículo 244.

acreditando su identidad y estado original, las condiciones y las personas que intervienen en la recolección, envío, manejo, análisis y conservación de estos elementos, así mismo, los cambios hechos en ellos por cada custodio; la cadena de custodia se inicia en el lugar donde se recaude el elemento físico de prueba y finalizará por orden de la autoridad competente[31].

Todos los servidores públicos y particulares que tengan relación con RF y EMP serán responsables de la aplicación de la cadena de custodia, dejando constancia escrita sobre y discriminada de acciones y elementos relacionados con el caso. Adicionalmente, el fiscal General reglamentará el diseño, aplicación y control del sistema de cadena de custodia, conforme con los avances científicos y técnicos del momento[32].

Finalmente, dentro de la ley 600 se considera el término "flagrancia" cuando la persona es sorprendida realizando una conducta punible, en dicho caso la persona será aprehendida junto con en material probatorio vinculado al hecho[33].

Ahora, centrando la atención sobre ley 906 de 2004 decretada por el Congreso de la República[34], en ella se menciona que la Fiscalía tiene la atribución para ordenar registros, allanamientos, incautaciones e interceptaciones de comunicaciones, y poner a disposición del juez de control de garantías el material probatorio recolectado. A su vez, la Fiscalía deberá asegurar los elementos materiales probatorios y evidencia física, garantizando su cadena de custodia; adicionalmente, deberá velar por la protección de las víctimas, testigos y peritos que la Fiscalía pretenda presentar.

Para dicho fin, la Fiscalía podrá solicitar al juez de control de garantías las medidas necesarias que aseguren la conservación de la prueba y la protección las víctimas[35].
Por otra pare cuando en ejercicio de la actividad de policía se descubran elementos materiales probatorios y evidencia física dentro de una diligencia,

---

[31] Ibid., Capítulo VIII, Artículo 288.

[32] Ibid., Capítulo VIII, Artículo 288.

[33] Ibid., Capítulo III, Artículo 345.

[34] --------. Ley 938. (30, Diciembre, 2004). Por la cual se expide el Estatuto Orgánico de la Fiscalía General de la Nación. Bogotá, D.C., 2004. no 45778. Disponible en Internet: http://www.fiscalia.gov.co/en/wp-content/uploads/2012/01/Ley938-de-2004.pdf

[35] Ibid., Capítulo I, Artículo 114.

estos serán responsables de recoger y embalar técnicamente los indicios y posteriormente comunicar el hallazgo a la policía judicial quien recogerá los elementos y el informe realizado .

La ley 906 también hace referencia a cuidados a tener en cuenta en el lugar de los hechos, menciona que una vez se tenga conocimiento de la comisión de un hecho que pueda constituir un delito, el servidor de policía judicial se trasladará al lugar de los hechos y lo examinará minuciosa, completa y metódicamente, con el fin de 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[36].

Antes de recoger el material encontrado, se deberá dejar evidencia fotográfica, de video o de cualquier otro medio técnico y se levantará el respectivo plano. En este punto la ley hace mención a que la Fiscalía deberá disponer de protocolos a seguir en la acción desarrollada, haciendo alusión a procedimientos para cadena de custodia[37].

Si el hecho punible se efectúa utilizando redes de telecomunicaciones, se ordenará a policía judicial la retención, aprehensión o recuperación de dicha información, equipos terminales, dispositivos o servidores que pueda haber utilizado cualquier medio de almacenamiento físico o virtual, análogo o digital, para que expertos en informática forense, descubran, recojan, analicen y custodien la información que recuperen[38].

Con el fin de demostrar la autenticidad de los elementos materiales probatorios y evidencia física, la cadena de custodia se aplicará teniendo en cuenta factores como 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[39].

[36] Ibid., Capítulo II, Artículo 213.

[37] Ibid., Capítulo II, Artículo 213

[38] Ibid., Capítulo V, Artículo 254.

[39] Ibid., Capítulo V, Artículo 254.

Cabe destacar que el servidor público en investigación policial embale y rotule el elemento material probatorio y evidencia física, será el responsable de su custodia y traslado al laboratorio correspondiente[40].

Cuando un perito que reciba algún contenedor con material probatorio, dejará constancia del estado en que se encuentra y procederá a las investigaciones y su respectivo análisis para la entrega final del informe. Cabe mencionar que cualquier persona vinculada a la investigación, antes de recibir material probatorio y evidencia física, deberá revisará el recipiente que lo contiene y dejará constancia del estado en que se encuentre[41].

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 y su legalidad depende de que en la diligencia en la cual se obtiene, se cumpla con la normatividad colombiana[42].

Identificación técnico científica. La identificación técnico científica consiste en la determinación de la naturaleza y características del elemento material probatorio y evidencia física, hecha por expertos en ciencia, técnica o arte. Dicha determinación se expondrá en el informe pericial[43].

El elemento material probatorio y evidencia física, recogidos por agente encubierto o en desarrollo de entrega vigilada, tiene el valor de cualquier otro elemento material probatorio y evidencia física siempre y cuando se establezca su autenticidad y se compruebe su correcta cadena de custodia[44].

El elemento material probatorio y evidencia física remitidos por autoridad extranjera, en desarrollo de petición de autoridad penal colombiana, será sometido a cadena de custodia y tendrá el mismo valor que se le otorga a cualquier otro elemento material probatorio y evidencia física[45].

---

[40] Ibid., Capítulo V, Artículo 258.

[41] Ibid., Capítulo V, Artículo 260.

[42] Ibid., Capítulo Único, Artículo 277.

[43] Ibid., Capítulo Único, Artículo 278.

[44] Ibid., Capítulo Único, Artículo 279.

[45] Ibid., Capítulo Único, Artículo 281.

En Colombia existe un bien jurídico denominado “de la protección de la información y de los datos”, ley 1273 de 2009 del Congreso de la República[46], ley que pretende la preservación integral de los sistemas que utilicen las tecnologías de la información y las comunicaciones, dictaminando penas por conductas punibles como el acceso abusivo a un sistema informático, la obstaculización ilegítima de un sistema informático o red de telecomunicación, la interceptación ilícita de datos informáticos, daños informáticos no autorizados, uso de software malicioso, violación de datos personales y suplantación de sitios web para capturar datos personales.

Dentro del Código Penal Colombiano[47] se encuentra la ley 599 del 2000 que trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones. Esta ley considera como delito sustraer, ocultar, extraviar, destruir, interceptar, divulgar, controlar o impedir una comunicación privada sin previa autorización, así mismo, se considera delito la utilización y tráfico de instrumentos para la interceptación de comunicaciones sin una autorización de las autoridades competentes o la utilización de equipos transmisores o receptores de señal con fines ilícitos.

Profundizando en el tema, en el artículo 15 de la Constitución[48] se estipula que toda persona tiene derecho a conocer, actualizar y rectificar la información que se haya recogido sobre ella en bancos de datos y en archivos de entidades públicas y privadas.

Adicionalmente dicho artículo menciona que la correspondencia y demás formas de comunicación privada son inviolables, estas solo podrán ser interceptadas o registradas mediante orden judicial y con las formalidades que establezca la ley.
Adicionalmente, en las leyes 679 y 1336 de 2009 del Congreso de la República[49], se afianza la lucha contra la explotación, la pornografía y el

[46] --------. Ley 1273. (5, Enero, 2009). Por la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y delos datos”. Diario Oficial. Bogotá, D.C., 2009. no 47223. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[47] --------. Ley 599. (24, Julio, 2000). Por la cual se expide el Código Penal. Diario Oficial. Bogotá, D.C., 2000. no 44097. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

[48] REPÚBLICA DE COLOMBIA. ASAMBLEA NACIONAL CONSTITUYENTE. Capítulo 6, Artículo 15, Artículo 250. Constitución Política de Colombia. Bogotá, D.C., 1991. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4125

[49] REPÚBLICA DE COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1336. (21, Julio, 2009). Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. Diario Oficial.

turismo sexual, con niños, niñas y adolescentes, decretando que todo aquel que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, trasmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años de edad, será castigado por la ley.

6.2.2 Límite de las competencias

Cualquier servidor designado para el manejo de la diligencia no deberá tomar acciones más allá de sus competencias.

Cada experto que tenga contacto con dispositivos de almacenamiento pendrive vinculados a un caso de informática forense deberá realizar las funciones asignadas sin extralimitarse y mucho menos si no se cuenta con una autorización ni conocimientos suficientes para realizar medidas adicionales.

6.2.3 Captura de Imágenes de un Dispositivo Pendrive

Para dar inicio al proceso de adquisición de imágenes de los dispositivos de almacenamiento pendrive USB, se debe preparar un laboratorio de software de análisis con características que permitan obtener, analizar y asegurar la evidencia digital.

Es indispensable contar con software especializado para la realización de esta tarea, teniendo en cuenta que no se podrá realizar modificación alguna ni dejar rastro sobre los datos que sean analizados, que por ningún motivo se modifiquen los tiempos de acceso o timestamp de los archivos del dispositivo origen.

Es necesario contar con un bloqueador de escritura que permita una conexión segura del dispositivo de almacenamiento origen al equipo forense, evitando de esta manera el riesgo de modificación del estado inicial del medio de almacenamiento sometido al análisis. En el mercado existen bloqueadores diseñados exclusivamente para dispositivos de almacenamiento USB como por ejemplo el USB WriteBlocker de Ondata, el cual se crea pensando en investigadores que trabajen con imágenes.

Este equipo se conecta al dispositivo de almacenamiento USB protegiendo su contenido durante la investigación, para lo cual solo es necesario conectar el

---

Bogotá, D.C., 2009. no 47417. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36877

WriteBlocker al dispositivo sospechoso. Adicionalmente el dispositivo incluye una utilidad de software forense que permite ver información de los dispositivos conectados y guardar la información en formatos de texto comunes.

Al igual que este, hay varias herramientas bloqueadoras de escritura tanto de software como de hardware con funciones similares las cuales se pueden utilizar para el manejo de pendrive.

Se deben realizar un mínimo de dos imágenes del dispositivo inicial, las dos copias se realizarán desde el dispositivo original. Las imágenes se deberán almacenar en un disco duro previamente sanitizado, preferiblemente utilizar discos duros de estado sólido los cuales no poseen discos giratorios ni partes móviles que se puedan ver afectadas con el movimiento y vibraciones.

6.2.4 Documentación de los Procedimientos

Se documentará cada acción realizada desde la recolección del dispositivo de almacenamiento pendrive hasta la entrega final de evidencia ante los tribunales, teniendo en cuenta la documentación establecida por la Fiscalía General de la Nación para el manejo y control de evidencia dentro de una cadena de custodia.

El personal asignado deberá tener en cuenta el tiempo universal coordinado indicado por el Instituto Nacional de Meteorología de Colombia (http://horalegal.sic.gov.co/) en el momento de realizar la comparación con la hora del sistema en el cual se involucren dispositivos pendrive.

Conservar una copia detallada de cada caso en el cual se haya visto involucrado o en el cual haya tenido contacto con medios de almacenamiento pendrive vinculados a un determinado proceso. De preferencia almacenar la información en dos lugares diferentes y en dispositivos que eviten adulteración o pérdida de la información contenida. Colocar los dispositivos en un lugar seguro con acceso restringido.

6.2.5 Evitar las Modificaciones

Para evitar el daño o alteración del material probatorio contenido en un pendrive se trabajará únicamente sobre las imágenes creadas del dispositivo, adicionalmente se trabajará con aplicaciones previamente colocadas a prueba que garanticen que la información contenida en el dispositivo original no sufra cambio alguno.

Adicionalmente se debe generar una suma de comprobación de la integridad de cada copia creada mediante el empleo de funciones hash de tal manera que se pueda demostrar que cada imagen es una fiel copia de su original[50].

6.2.6 Desconectar los medios

Desconectar el cable de red e inactivar conexiones inalámbricas en equipos vinculados en la escena que tengan medios de almacenamiento USB conectados.

Si no se percibe una amenaza y el equipo en el cual se encuentra conectado el dispositivo de almacenamiento pendrive USB se encuentra encendido, se recomienda proceder a apagar el equipo para posteriormente retirar el pendrive, de no ser posible apagar el equipo, se debe realizar los procedimientos para la extracción segura del dispositivo y como opción final la extracción a la fuerza.

Tener en cuenta cualquier equipo relacionado en la escena el cual tenga conectados dispositivos de almacenamiento pendrive USB y se encuentre apagado, deberá mantenerse apagado, además será necesario elaborar un registro fotográfico del equipo, su localización y medios dispositivos pendrive a él conectados[51].

De ser necesario apagar el equipo al cual se encuentre conectado un pendrive, tener muy en cuenta antes de proceder con el apagado, contar con una previa autorización judicial, o en su defecto del o los propietarios o directrices de la organización, además de contar con el visto bueno administrador de los sistemas de cómputo; el apagar un equipo puede detener procesos y servicios vitales para una organización, causar pérdida de información, detención de la continuidad del negocio, generar perjuicios económicos entre otros. El contar con una previa autorización podrá evitar futuras sanciones legales.

[50] López Delgado, Miguel. Análisis Forense Digital 2 ed. Hackers y Seguridad: Junio, 2007. p. 16. Disponible en Internet: http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[51] ESTADOS UNIDOS DE AMÉRICA. DEPARTMENT OF HOMELAND SECURITY. Best Practices For Seizing Electronic Evidence a Pocket Guide for First Responders. 3 ed. Op. cit., p.7. Disponible en Internet: http://www.forwardedge2.com/pdf/bestpractices.pdf

Si el equipo involucrado está encendido, pero se está ejecutando software destructivo (formateo, borrado de la información, malware), su cable de poder debe ser desconectado de inmediato para preservar la evidencia[52].

Si el equipo está encendido, hay dos maneras para apagarlo:

1. Apagado forzado.

   Si el equipo está encendido y existe el riesgo de la destrucción de pruebas, se debe realizar un apagado forzoso tirando el cable de alimentación de la fuente de electricidad o quitar la batería de la computadora portátil[53].

   Antes de realizar este procedimiento, tener en cuenta que un apagado forzoso podrá:

- Preservar algunos archivos de sistema al interrumpir software de formateo o borrado de archivos.
- Prevenir la activación de programas destructivos.
- Evitar cambios en fecha y hora del equipo o de modificación de sus archivos.
- Evitará cambios a los atributos del archivo.
- El sistema operativo se podría dañar.
- Podrían afectarse documentos.
- Se podrían perder los archivos abiertos sin guardar.
- El equipo podría estar encriptado lo cual dificultaría en gran manera tener nuevamente acceso a la información[54] .

2. Apagado Ordenado.

   Con un cierre correcto, se apaga el sistema operativo de la manera recomendada por los fabricantes del software. Es importante tener en

[52] ESTADOS UNIDOS DE AMÉRICA. NATIONAL FORENSIC SCIENCE TECHNOLOGY CENTER NFSTC. Op. cit., p.7.

[53] --------. Digital Evidence field Guide: What Every Peace Officer Must Know. Op. cit., p. 15.

[54] Ibid., p.15.

cuenta que los métodos de cierre para varían según el sistema operativo. Tener en cuenta que un apagado ordenado podría:

- Ayudar a localizar las conexiones de red e Identificar y cerrar los archivos abiertos.
- Asegurar un futuro arranque exitoso del equipo.
- Perder algunos archivos de sistema si bajo plano se está ejecutando software destructivo o comandos de borrado de información.
- Activar programas destructivos al ejecutar la secuencia de comandos de cierre[55].

6.2.7 Recolección y Análisis

Se aplica a la escena del crimen. Primero se deberán buscar todas las fuentes de evidencia entre las cuales se encuentran los dispositivos de almacenamiento pendrive USB, una vez se constate que el proceso de recolección ha terminado, se procederá a un análisis pertinente de cada dispositivo encontrado.

6.2.8 Puesta a Prueba

Cada aplicación utilizada en la obtención de imágenes del pendrive original y creación de la firma hash, al igual que cada aplicación utilizada para el análisis de datos debió ser probada con anterioridad para demostrar su efectividad.

Adicionalmente, cada procedimiento que recaiga sobre el dispositivo de almacenamiento pendrive durante su proceso de cadena de custodia, también debió ser puesto a prueba con anterioridad.

6.2.9 Seguimiento de Directrices Establecidas

Se recomienda seguir las directrices propuestas en el Manual de Procedimientos Para cadena de Custodia de la Fiscalía y las directrices adoptadas por la institución a cual pertenece el investigador. Adicionalmente basar los procedimientos realizados sobre dispositivos de almacenamiento

[55] Ibid., p.15.

pendrive en la presente norma ISO/IEC 27037:2012 y sugerencias realizadas en el presente documento.

6.3 RECOLECCIÓN DE EVIDENCIA SEGÚN LA VOLATILIDAD

Para la recolección de evidencia se debe proceder teniendo en cuenta el nivel de volatilidad comenzando por la más a la menos volátil.

Para el caso de dispositivos de almacenamiento pendrive USB aplica a dichos dispositivos encontrados en la escena del crimen y que están conectados a algún equipo.

La norma ISO 27037 aclara que primero se debe proceder con la recolección de posible evidencia volátil en los registros, caché, tablas de enrutamiento, caché arp, la tabla de procesos, kernel y memoria del equipo. Posteriormente se pasará a recolectar posible información volátil contenida en discos y dispositivos de almacenamiento pendrive.

6.4 PARA CONSERVAR LA EVIDENCIA

Es muy fácil de destruir pruebas, aunque inadvertidamente, por esto se lista una serie de acciones que se deben evitar para evitar la pérdida de evidencia digital.

6.4.1 Antes de Apagar los Equipos

Aplica para los dispositivos informáticos encontrados en la escena del crimen en los cuales se encuentra conectado por lo menos un dispositivo de almacenamiento pendrive USB. Si en dichos equipos se corre alguna aplicación para la recuperación de evidencia, evidencia volátil, para la creación de imágenes en caliente, se deberá estar seguro que se rescató toda la información necesaria y que terminaron de ejecutarse todos los procesos ejecutados por las herramientas utilizadas por el investigador antes de proceder a apagar un equipo.

Usualmente los delincuentes informáticos desconectan abruptamente la fuente de energía pretendiendo con esta acción que el sistema operativo de los ordenadores pierda su secuencia de arranque y se destruyan los archivos de

registro de inicio de sesión y de programas que se estén ejecutando en el instante del delito y en raras ocasiones ocasionando daño en el disco duro, razón por la cual se considera necesario que el servidor designado, tome las medidas necesarias para que se restrinja el paso hacia tableros eléctricos o fuentes de alimentación de energía de los equipos de cómputo presentes en la escena en los cuales se involucren dispositivos pendrive mientras se realizan las acciones pertinentes.

6.4.2 Registro del tiempo de acceso

Por ningún motivo se deberá ejecutar programas, aplicaciones y comandos que afecten el estado inicial de la información contenida en un dispositivo de almacenamiento pendrive USB. Solo se utilizaran herramientas previamente probadas que aseguren que el estado inicial de los datos contenidos en el pendrive no sufrirá modificación alguna. Evitar el uso de 'tar' o 'xcopy'.

6.5 CONSIDERACIONES DE PRIVACIDAD

6.5.1 Normas y Directrices de la Empresa

El personal que de una u otra manera tenga acceso a la información contenida en dispositivos de almacenamiento pendrive USB relacionados con la cadena de custodia en un caso de informática forense, deberá ser ético y profesional con la información a la cual tenga acceso, no deberá comentarla, ni mucho menos copiarla para intereses personales. Adicionalmente se deberá tomar las medidas pertinentes para evitar que personas ajenas a la investigación tengan acceso dicha información. Por este motivo, cualquier dispositivo pendrive en el que se almacene la información recuperada debe ser almacenado en un lugar seguro con acceso restringid, un sistema que permita identificar los accesos no autorizados y adicionalmente registrar cada acceso autorizado a dichos dispositivos.

6.5.2 Respaldo de la Empresa

Se debe estar seguro de tener el respaldo de la empresa para realizar los procedimientos y medidas que permitan recopilar evidencia de un incidente.

Contar con una previa autorización judicial, o permiso de los propietarios o directrices de la organización, además de tener el visto bueno administrador de los sistemas de cómputo antes de realizar procedimientos de búsqueda de medios de almacenamiento pendrive USB y su posterior y análisis al contenido.

6.6 CARACTERÍSTICAS DE LA EVIDENCIA DIGITAL CONTENIDA EN UN PENDRIVE

6.6.1 Admisible

Para poder presentar evidencia admisible recolectada de dispositivos de almacenamiento pendrive USB ante un tribunal, esta debió ser adquirida por medio de procedimientos que acataron la normatividad colombiana citada en el numeral 5.2 del presente documento y a cualquier otra norma de la constitución de Colombia referente al manejo de evidencia digital y cadena de custodia.

6.6.2 Auténtica

Para lograr una autenticidad del material probatorio recolectado de un dispositivo de almacenamiento pendrive USB, debe existir documentación acreditada de cada proceso realizado sobre el dispositivo y registros fotográficos con firma hash. Adicionalmente la función hash del dispositivo original y de sus imágenes podrá vincular con la fuente la evidencia recolectada.

Por otra parte, el análisis a la evidencia recolectada del dispositivo pendrive deberá recolectar material probatorio contundente que relacione al delincuente con el delito cometido y con el lugar de los hechos.

6.6.3 Completa

El experto que analice la información contenida en el dispositivo pendrive tomará las medidas respectivas para recuperar la mayor cantidad de material probatorio que permita explicar el hecho punible.

6.6.4 Confiable

No debe generar duda alguna sobre la autenticidad, veracidad y la transparencia de la evidencia desde su recolección, manejo durante el proceso de cadena de custodia, hasta su entrega final ante un tribunal.

Por medio de los procedimientos propuestos en el presente trabajo para acatar la norma ISO 27037 se pretende generar evidencia confiable y fácilmente autenticable ante un tribunal.

Adicionalmente las herramientas utilizadas van a permitir generar los mismos resultados al ser aplicadas bajo los mismos dispositivos.

6.6.5 Creíble

Para la realización de informes finales, los expertos que recolectaron la evidencia encontrada en los dispositivos de almacenamiento pendrive, deberán evitar en lo posible la utilización de tecnicismos de tal manera que su explicación escrita y verbal sea comprensible en un tribunal.

6.7 PROCEDIMIENTO DE ASEGURAMIENTO DE LA EVIDENCIA DIGITAL EN UN PENDRIVE

Cada funcionario que tenga contacto en alguna de las fases de cadena de custodia en la que intervenga un dispositivo de almacenamiento pendrive deberá documentar todo procedimiento que se realice al dispositivo mientras se encuentre bajo su custodia, documentar el estado en el cual se recibe, el estado en el cual se entrega y diligenciar cada uno de los documentos destinados por la Fiscalía.

6.7.1 Procedimientos Para la Cadena de Custodia de un Dispositivo Pendrive

- Dónde, cuándo y por quién fue descubierta y recogida la evidencia.
- Dónde, cuándo y por quién manipuló o examinó la evidencia.
- Quién tenía la custodia de las evidencias y durante qué período.

- Cómo fue almacenada la evidencia.
- Cuando la evidencia cambió de custodia, cuándo y cómo se hizo la transferencia (incluyen los números de envío, etc).

6.7.2 Procedimiento Para el Almacenamiento de un Dispositivo Pendrive

De ser posible, los medios los medios físicos se deben almacenar en un lugar oscuro, adicionalmente el lugar de almacenamiento que contenga los dispositivos de almacenamiento debe ser seguro, estar libre de señales electromagnéticas, humedad y altas temperaturas[56].

Como parte del sistema de seguridad, los depósitos de evidencias que contengan dispositivos de almacenamiento pendrive USB deberán contar con un custodio permanente las 24 horas del día, en turnos de 8 horas, cubiertos por funcionaros de la institución o por servicio de guarda de seguridad privada[57].

El almacén de evidencias deberá contar con sistemas de detección y combate contra incendios, tales como detectores de última generación, sistema de extinción, bocas de incendios equipadas, bocas de incendio siamesas, extintores portátiles de incendio diferenciados, sensores de humo y calor, termo velocímetro y carteles señalizadores[58].

El almacén que contenga material probatorio deberá contar con un circuito cerrado de televisión tanto en el interior como en la seguridad perimetral externar. Además, contar con una sala de monitoreo central en la cual se alberguen los dispositivos de control de las cámaras de circuito cerrado de televisión, sensores de movimiento, de intrusismos, control de bombas de incendio entre otros[59].

---

[57] REPÚBLICA DE PARAGUAY. MINISTERIO PÚBLICO. Depósito Modelo de Evidencia. Estrictos Protocolos de Procedimientos y Tecnología de Punta. Op. cit., p. 7.

[58]Ibid,, p. 17- 18.

[59] Ibid., p. 7.

6.8 HERRAMIENTAS PARA LA RECOLECCIÓN Y MANEJO DE EVIDENCIA VINCULADA A UN DISPOSITIVO PENDRIVE

Se debe tener los programas que necesarios para realizar la recopilación de pruebas en medios de sólo lectura, así como el conjunto de herramientas para cada uno de los sistemas operativos que a los cuales se vaya a tener acceso, entre los cuales se destaca:

- Un programa para el examen de los procesos (por ejemplo, 'ps').

  Se trata de un comando de Unix y Linux que sirve para mostrar información sobre procesos que se están ejecutando en el sistema.

- Programas para examinar el estado del sistema (por ejemplo, 'showrev', 'ifconfig', 'netstat', 'arp').

  Comando showrev. Este comando permite visualizar en Unix y Linux características del software y hardware actual en el equipo, como por ejemplo la versión, el hostname, hostid y la arquitectura.

  Comando ifconfig. Es un comando de Unix y Linux que permite visualizar y configurar las interfaces de red en el equipo.

  Comando netstat. Es un comando de Windows que permite conocer información sobre las conexiones establecidas por el equipo por medio de los puertos abiertos, conexiones en segundo plano, e incluso puede indicar conexiones establecida por programas espía.

  Comando arp. Este comando muestra entradas en la caché permitiendo su modificación. Contiene tablas que se utilizan para almacenar las direcciones IP y las direcciones físicas ethernet.

- Un programa para hacer copias bit a bit (por ejemplo, 'DD', 'SafeBack').

  Comando dd. Es un comando de Unix y Linux que permite crear imágenes de discos bit a bit, además de ofrecer otras opciones como obtención del hash MD5 de la copia.

  SafeBack. Aplicación que permite crear una imagen espejo bit a bit de un disco, una unidad de disco y de unidades de almacenamiento de información.

- Programas para generar sumas de comprobación y firmas (por ejemplo, 'sha1sum', un 'dd' checksum, 'SafeBack").

  Comando sha1sum. Es un comando de Unix y Linux que permite identificar la integridad de un archivo mediante la suma de comprobación del hash.

  Comando dd. Además de permitir la creación de imágenes bit a bit, dd tiene la opción de generar sumas de comprobación hash de los archivos e imágenes creadas.

  Cheksum. Es una función hash que permite verificar cambios en la secuencia de datos de un archivo.

  SafeBack. Además de permitir la creación de imágenes bit a bit, SafeBack tiene la opción de generar sumas de comprobación hash de los archivos e imágenes creadas.

7. CONCLUSIONES

Por medio del estudio de la Norma ISO/IEC 27037:2012 se identificaron lineamientos sobre los cuales fue viable incorporar procedimientos para el manejo de evidencia digital contenida en dispositivos de almacenamiento pendrive USB. Dichos procedimientos aunque son ajenos a la ISO 27037, se plantearon de tal manera que permitieron explicar parte del contenido de la norma y adicionalmente se manejaron como texto de ayuda y a la norma y al lector que en un futuro decida comprobar su aplicabilidad en el campo de la práctica.

Adicionalmente, el desarrollo del trabajo proporcionó una serie de explicaciones sobre el contenido de la norma ISO/IEC 27037:2012 aplicadas al manejo de evidencia digital contenida en dispositivos de almacenamiento pendrive. Las explicaciones proporcionadas surgen del estudio realizado a dicha norma, arrojando como un hecho palpable que la norma ISO 27037:2012 es viable para el tratamiento y aseguramiento de la evidencia digital contenida en dispositivos de almacenamiento pendrive USB.

Como complemento, se logra Identificar que aunque la norma ISO/IEC:2012 fue creada pensando en una normatividad internacional estándar, es flexible ante la normatividad colombiana vinculada directa o indirectamente con el manejo de evidencia digital presente en dispositivos de almacenamiento pendrive USB. Adicionalmente la norma ISO 27037 avala a los servidores públicos para el manejo de evidencia digital siempre y cuando Constitución acredite al servidor para el manejo de dicha responsabilidad.

8. RECOMENDACIONES

Una vez concluida la presente monografía se recomienda:

- Utilizar la Norma ISO/IEC 27037:2000 para casos de informática forense en los cuales intervenga uno o más dispositivos de almacenamiento digital de tipo pendrive USB.

- Si para casos de informática forense en los que intervengan dispositivos de almacenamiento de tipo pendrive USB se planea utilizar procedimientos adicionales que no se encuentren en la norma ISO/IEC 27037, se recomienda validar primero dichos procedimientos antes de su aplicación.

BIBLIOGRAFÍA

ALMEIDA ROMO, Omar Ramiro. Metodología para la implementación de informática forense en sistemas operativos Windows y Linux. Trabajo de Grado. Ibarra: Universidad Técnica del Norte. Facultad de Ingeniería en Ciencia Aplicadas, 2011. p. 33-36. Consultado En: http://repositorio.utn.edu.ec/bitstream/123456789/539/7/04%20ISC%20157%20CAPITULO%20II.pdf

ÁLVAREZ DAVID, Paula Andrea. Análisis Jurídico y Material de la Evidencia Digital en los Delitos Informáticos Judicializados por la Fiscalía General de la Nación en el Municipio de Bucaramanga en el Periodo 2006-2010. Tesis. Bucaramanga: Universidad Pontificia Bolivariana, Escuela de Derecho y Ciencias Políticas, Diciembre, 2011. p. 12-16, 68-76, 80. Consultado en: http://repository.upb.edu.co:8080/jspui/bitstream/123456789/1834/1/digital_22203.pdf

BRENZINSKI, KILLALEA. Guidelines for Evidence Collection and Archiving RFC 3227. Neart.org, 2002.p.1-10.

CABRERA MESA, Harold Emilio, ing. esp.. Informática Forense, Unidad 1. Fundamentos de la Informática Forense. Pasto: Universidad Nacional Abierta y a Distancia, UNAD, 2013. p. 3. Disponible en Internet: http://datateca.unad.edu.co/contenidos/233012/unidad_1/u1_introduccion%20a%20la%20informatica%20forense.pdf

CAMPOLI, Gabriel. Manual Básico de Cateo y Aseguramiento de Evidencia Digital. En: Revista de Derecho Informático. 2006, no 99. p. 3-8.

CASEY, E. Digital Evidence and Computer Crime. Citado por CANO, Jeimy. Admisibilidad de la Evidencia Digital: De los conceptos legales a las Características Técnicas. Trabajo de grado. Bogotá D.C.: Universidad de Los Andes. Facultad de Derecho, 2003. p.2. Disponible en Internet:

file:///C:/Users/Jose/Downloads/EJUS_BOGOTA_2007_EVIDENCIA_DIGITAL_EN_COLOMBIA.pdf

CENTRO INTERACTIVO DE CIENCIA Y TECNOLOGÍA HORNO3. Divulgación de la Ciencia. Boletín 58. Monterrey: 2013. Disponible en Internet: horno3.ensi.com.mx/apps/newsletter/idem.php?module=Newsletter&action=ReadNewsletter&newsletter_id=4782

DIVISIÓN FORENSE. PRODUCTOS E INSUMOS DE CRIMINALÍSTICA. Bolsa de Faraday Para Dispositivos Móviles. Buenos Aires: División Forense, 2014. Disponible en Internet: https://www.division-forense.com/bolsa-faraday.html

--------. Best Practices For Seizing Electronic Evidence a Pocket Guide for First Responders. 3 ed. Washinton: El Departamento, s.f. p. 3-4, 7. Disponible en Internet: http://www.forwardedge2.com/pdf/bestpractices.pdf

ESTADOS UNIDOS DE AMÉRICA. DEPARTMENT OF JUSTICE. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Washington: El Departamento, 2002. Citado por GHOSH, Ajoy. Incident Response and Forensics Workshop. Doc No: telwg29/IRF/04a, Australia: Guidelines for the Management of IT Evidence, 2004. p. 10.

--------. Digital Evidence field Guide: What Every Peace Officer Must Know. Washington: La Oficina, s.f. p. 2-4, 10, 14-16.

ESTADOS UNIDOS DE AMÉRICA. NATIONAL FORENSIC SCIENCE TECHNOLOGY
CENTER NFSTC. A Simplified Guide to Digital Evidence. Florida: El Centro, 2012. p. 3, 6-7, 22.

GALEANO MARÍN. María Eumelia. Diseño de proyectos en la investigación cualitativa. Medellín: Universidad EAFIF, 2004. Disponible en Internet: http://bienser.umanizales.edu.co/contenidos/lic_ingles/fundamentos_teoricos/criterios_conceptuales/recursos_estudio/pdf/INVESTIGATIVO/EL%20CAMBIO%20DEL%20ENFOQUE%20INVESTIGATIVO.swf

--------. Manual de Buenas Prácticas en la Escena del Crimen, AICEF/GITEC. 1 ed. México, D.F.: Instituto Nacional de Ciencias Penales, 2010. p. 11-17, 23-29, 42, 70.

GOBIERNO DE ESPAÑA. MINISTERIO DE ECUACIÓN, CULTURA Y DEPORTE. Usos Avanzados de una Memoria USB. Disponible en Internet: http://recursostic.educacion.es/observatorio/web/eu/equipamiento-tecnologico/hardware/703-usos-avanzados-de-una-memoria-usb

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. Cómo Comprobar la Integridad de los Ficheros. INTECO: Madrid, s.f. p. 2-3.

JOYA RAMIREZ, Nohora, et al. Guía Para la Elaboración de Trabajos Escritos, Sexta Actualización. Bogotá, D.C.: ICONTEC, 2013. p. 9- 219.

LIMA MALVIDO, María de la Luz. Delitos electrónicos. Ciudad Capital: Academia Mexicana de Ciencias Penales, 1984. p. 100.

--------. Standards Catalogue ISO/IEC 27037:2012. Genova: ISO, 2012. Disponible en Internet: www.iso.org/iso/catalogue_detail?csnumber=44381

PRIETO, Diana, Moreno, Claudia. Evidencia Digital en Colombia: Una reflexión en la práctica. En Revista de Derecho Informático. Abril, 2007, no. 107. p. 1-8.

REPÚBLICA DE COLOMBIA. ASAMBLEA NACIONAL CONSTITUYENTE. Capítulo 6, Artículo 15, Artículo 250. Constitución Política de Colombia. Bogotá, D.C., 1991. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4125

REPÚBLICA DE COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 489. (29, Diciembre, 1998). Por la cual se dictan normas sobre la organización y funcionamiento de las entidades de orden nacional. Diario Oficial. Bogotá, D.C., 1998. no 43464. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=186

--------. Ley 599. (24, Julio, 2000). Por la cual se expide el Código Penal. Diario Oficial. Bogotá, D.C., 2000. no 44097. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

--------. Ley 600 de 2000. (24, Julio, 2000). Formula que toda investigación debe fundarse en pruebas legales oportunamente vinculadas a la actuación. Diario Oficial. Bogotá, D.C., 2000. no 44097. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6389

--------. Ley 678. (3, Agosto, 2001). Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores. Diario Oficial. Bogotá, D.C., 2001. no 44509. Disponible en Internet: file:///C:/Users/user/Downloads/LEY%20678%20DEL%203%20DE%20AGOSTO%20DE%202001.pdf

--------. Ley 906. (1, Enero, 2005). Formula que la Fiscalía tiene la atribución para ordenar registros, allanamientos, incautaciones e interceptaciones de comunicaciones. Diario Oficial. Bogotá, D.C., 2005. no 45658. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=14787

--------. Ley 1273. (5, Enero, 2009). Por la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la

protección de la información y delos datos". Diario Oficial. Bogotá, D.C., 2009. no 47223. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

--------. Ley 1336. (21 Julio, 2009). Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. Diario Oficial. Bogotá, D.C., 2009. no 47417. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36877

REPÚBLICA DE COLOMBIA. CORTE CONSTITUCIONAL. Sentencia C-662/00. (8, Junio, 2000). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Expediente. Bogotá, D.C., 2009. no D-2693. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5789

REPÚBLICA DE COLOMBIA. FISCALÍA GENERAL DE LA NACIÓN. Manual de Procedimientos Para Cadena de Custodia. Introducción. Bogotá: La Fiscalía, 2005. p. 1-147.

--------. Resolución 000435. 1 EF. (1, Enero, 2005). Por la cual se hace entrega del "Manual de Procedimientos Bodega de Evidencias ". Bogotá, D.C., 2005. p. 19. Disponible en Internet: http://criminalistica-odg.wikispaces.com/file/view/manual+de+Procedimiento+de+evidencias.pdf

--------. Resolución 0-1890. (5, Noviembre, 2002). Por medio de la cual reglamenta el artículo 288 de la ley 600. Bogotá, D.C., 2002.

--------. Resolución 0-2869. (29, Diciembre, 2003). Por medio de la cual se adopta el Manual de Procedimientos del Sistema de Cadena de Custodia. Bogotá, D.C., 2003. Disponible en Internet: http://www.medellin.gov.co/transito/archivos/normatividad/resoluciones_nacionales/2003/2003-resolucion2869.pdf

--------. Resolución 0-6394. (22, Diciembre, 2004). Por medio de la cual se adopta el manual de procedimientos del Sistema de Cadena de Custodia para el Sistema Penal Acusatorio. Diario Oficial. Bogotá, D.C., 2004. no 45772. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=15634

REPÚBLICA DE COLOMBIA. LA SALA ADMINISTRATIVA DEL CONSEJO SUPERIOR DE LA JUDICATURA. Acuerdo PSAA06-3334. (2, Marzo, 2006). Por el cual se reglamentan la utilización de medios electrónicos e informáticos en el cumplimiento de las funciones de administración de justicia. Bogotá, D.C., 2006. p. 6. Disponible en Internet: http://programa.gobiernoenlinea.gov.co/apc-aa-files/92e2edae878558af042aceeafd1fc4d8/ejus_csdj_2006_acuerdo_3334.pdf

REPÚBLICA DE COLOMBIA. POLICÍA NACIONAL. Criminalística de Campo. Bogotá, D.C.: Escuela de Investigación Criminal, 2011. p. 9, 15. Disponible en Internet: http://www.policia.edu.co/documentos/ascensos/pt_a_si/ayudas/PRESENTACION%20PRIMER%20RESPONDIENTE.pdf

--------. Decreto 1360. (23, Junio, 1989). Por el cual se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor. Bogotá, D.C., 1989. p. 3. Disponible en Internet: http://www.viceinvestigacion.unal.edu.co/VRI/files/propiedad_intelectual/decreto_1360.pdf

--------. Decreto 1747. (11, Septiembre, 2000). Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales. Diario Oficial. Bogotá, D.C., 2000. no 44160. Disponible en Internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4277

REPÚBLICA DE PARAGUAY. MINISTERIO PÚBLICO. Depósito Modelo de Evidencia. Estrictos Protocolos de Procedimientos y Tecnología de Punta. Asunción: El Ministerio, 2010. p. 7. 17-18.

SELLTIZ, Claire, et al. Métodos de Investigación de la Relaciones Sociales.
9. ed. Madrid: Ediciones Rialp, 1980.

TAMAYO, PABLO. Tutorial, citado por Lituma, Marco. Criptografía: Funciones Hash como alternativa de seguridad en Transacciones Online para Organizaciones o Empresas. Sf. p. 25-26.

TORRES, Daniel; CANO, Jeimy; RUEDA, Sandra. Evidencia Digital en el Contexto Colombiano: Consideraciones Técnicas y Jurídicas Para su Manejo. ACIS. 2006. Disponible en Internet: http://www.acis.org.co/index.php?id=856

UYANA GARCÍA, Mónica Alexandra, Ing. Diseño de un Área Informática Forense para un Equipo de Respuestas Ante Incidentes de Seguridad Informáticos CSIRT. Tesis de grado. Sangolquí: Universidad de las Fuerzas Armadas ESPE del Ecuador. 2014. p. 233.