Buenas prácticas en informática forense, para el procesamiento de evidencia digital o información electrónicamente almacenada

Good practices in computer forensics for the processing of digital evidence or electronically warehouse information

César Arturo Contreras Calderón

Universidad Nacional Abierta y a Distancia, Profesional especializado en Informática Forense.

Recibido: 15/10/ 2021 Aprobado 10/12/2021

Resumen

El presente artículo responde a la necesidad de construir buenas prácticas en ambientes y escenarios informáticos para el procesamiento de evidencia digital, que fortalezca las capacidades técnico científicas del investigador y/o perito público o privado, para la obtención de resultados positivos frente al tratamiento del elemento material probatorio y/o evidencia física (Congreso de la República, 2004) que se hallen en el lugar de los hechos, que por su naturaleza digital o electrónica requiera de un embalaje especial. Así mismo, que el practicante mediante la aplicación de una metodología adecuada perfeccione el procedimiento de embalaje y sometimiento del mismo al protocolo establecido de cadena de custodia (Fiscalía General de la Nación, 2016), independientemente del lugar en que se recolecte, se deben aplicar los principios de mismidad, autenticidad y originalidad. Se espera que el lector tenga facilidad de identificar los materiales que pueden utilizar para la fabricación de un contenedor cuya utilidad se destine al embalaje de evidencia digital o información almacenada electrónicamente (Withers, s.f.).

Palabras clave: informática forense, embalaje, contenedor, evidencia digital, información almacenada electrónicamente, metodología.

Resumen

This article responds to the need to build good practices in computer environments and scenarios for the processing of digital evidence, which strengthens the scientific technical capacities of the researcher and / or public or private expert, to obtain positive results against the treatment of the element probative material and / or physical evidence (Congreso de la República, 2004) found at the scene, which due to its digital or electronic nature requires special packaging. Likewise, the practitioner, through the application of an adequate methodology, perfect the packaging procedure and submitting it to the established chain of custody protocol (Fiscalía General de la Nación, 2016), regardless of the place

Citación: Contreras Calderón, C. A. (2022). BUENAS PRÁCTICAS EN INFORMÁTICA FORENSE PARA EL PROCESAMIENTO DE EVIDENCIA DIGITAL O INFORMACIÓN ELECTRÓNICAMENTE ALMACEN. Publicaciones E Investigación, 15(2). https://doi.org/10.22490/25394088.5245

cacontrerasca@unadvirtual.edu.co, https://orcid.org/0000-0003-0407-2063

https://doi.https://doi.org/10.22490/25394088.5245

where it is collected, the principles of sameness, authenticity and originality. It is expected that the reader will be able to identify the materials that they can use for the manufacture of a container whose utility is destined to the packaging of digital evidence or information stored electronically (Withers, s.f.).

Keywords: *Computer Forensics, packaging, container, digital evidence, electronically stored information, methodology.*

1. Introducción

El propósito general de este artículo es brindar un conocimiento teórico práctico para el desarrollo de habilidades adecuadas en relación a la elaboración de contenedores para el embalaje de evidencia digital o información almacenada electrónicamente, con el fin de que el investigador o perito, independientemente del cargo que desempeñe, pueda realizar buenas prácticas al momento de recolectar el elemento material probatorio o evidencia física, que por su naturaleza digital o electrónica requiera que se conserve en un ambiente propio a su clasificación. Teniendo en cuenta de no incurrir en los principios de confidencialidad, integridad y disponibilidad (Icontec, 2013) para el tratamiento de información. Aunado a esto, se deben utilizar los protocolos de cadena de custodia al momento de realizar la identificación y recolección del mismo. Por lo anterior es necesario que el practicante tenga la habilidad de utilizar los materiales adecuados para la elaboración del contenedor en cualquier escenario que se requiera y que por diferentes razones no cuente con una bolsa antiestática, en aras de aislar el dispositivo de cualquier señal o frecuencia que interrumpa el procedimiento y ponga en riesgo la integridad de la evidencia (fuentes de datos).

Simultáneamente, se identifica uno de los muchos problemas al que se enfrenta un investigador cibernético o un perito informático dentro de una organización o entidad estatal, y es la dependencia financiera, la cual limita el desarrollo de la actividad forense. En consecuencia, el funcionario a la hora de realizar el procedimiento de recolección y embalaje de la evidencia, se da a la tarea de utilizar los medios existentes para dar cumplimiento a su deber, pero no en muchos casos resulta ser la mejor elección, debido a que la evidencia termina siendo manipulada de manera accidental, lo que implica un riesgo para la información, toda vez que pasa por alto los principios de cadena de custodia al no haber utilizado un contenedor adecuado para el embalaje de la evidencia digital.

En la actualidad, los escenarios a los que se enfrenta un investigador o perito informático, van más allá de lo que en tiempos anteriores se trataba de un simple problema tecnológico, toda vez que la mutación del delito en materia informática evoluciona, creando nuevas técnicas antiforense para destruir, ocultar, eliminar o falsificar la evidencia digital. Dadas las circunstancias en cómo se inicia el procedimiento legal para poder obtener una prueba de una evidencia digital, es necesario que el procedimiento para la preservación del mismo sea lo más trasparente y meticuloso posible, con el objetivo de no dejar vacíos jurídicos, que afecten el proceso investigativo y exoneren de toda responsabilidad al autor o participe de los hechos.

En la manipulación de pruebas digitales, las acciones que se lleven a cabo no deben alterar dicha prueba (Rosado, 2011), consagrado esto desde la óptica de los principios aplicables a los procedimientos que tuvo sus inicios en el siglo XXI, con el primer informe presentado por el grupo de Lyón (Pollitt, 2001) perteneciente a la IOCE (Organización Internacional de Evidencia Computacional) FBI 1990, donde se llegó a pensar por primera vez en la necesidad de poder estandarizar una serie de buenas prácticas para el proceso forense en el manejo de la evidencia digital, es allí donde por parte del G8 (un grupo de ocho países con economías

industrializadas del planeta) aprueban la propuesta para formalizar dichos principios, cuya finalidad es poder salvaguardar el procedimiento forense en relación al tratamiento de evidencia digital. Por esta razón es indispensable replicar estos principios que fueron adoptados por las diferentes entidades policiales alrededor del mundo, implementado controles adecuados para no irrumpir el proceso judicial con malas prácticas que lleguen a invalidar la prueba.

Dentro del accionar delincuencial frente a la comisión de un delito informático, se busca como objetivo lograr ocultar los rastros de las huellas digitales que puedan ser parte de una investigación, debido a lo cual es la importancia de no permitir que la evidencia pueda ser borrada o en su defecto modificada.

Ahora bien, de lo que se trata es de garantizar el continuo desarrollo del proceso judicial frente a cualquier análisis contra pericial por parte de la defensa técnica, quien a su vez busca de manera concienzuda lograr exonerar de responsabilidad al delincuente, mediante la desacreditación del procedimiento forense por parte del ente acusador, sin embargo, la existencia de buenas prácticas en el paso a paso para desarrollar la investigación criminalística, aseguran mayor grado de certeza y probabilidad al análisis de la evidencia, que a su vez se convertirá en una prueba dentro de un estrado judicial, si logra sustentar que efectivamente el elemento se le respetaron sus principios de cadena de custodia.

Nota: la metodología que se aplica para el desarrollo de las buenas prácticas, no está sujeta a que el practicante tenga que pertenecer a alguna entidad estatal para ser implementada, sino por el contrario se generaliza a la necesidad del caso, toda vez que una persona sin conocimientos técnicos pueda realizarla sin ninguna dificultad.

1.1 Riesgo

Se plantea de manera ordenada y estructurada el desarrollo metodológico, en el cual se identifican los diferentes dispositivos electrónicos de almacenamiento digital que puedan estar involucrados en una escena criminal. Aunado a esto, los riesgos a los que se expone la evidencia digital y cómo prevenirlos, así mismo, se muestra la elaboración de un contenedor para el embalaje de evidencia digital, encaminado a generar buenas prácticas en el campo de la informática forense.

Listado de dispositivos o aparatos electrónicos, que por su naturaleza almacenan datos digitales y pueden ser objeto de recolección en un lugar de los escenarios criminales:

Disco duro	Memoria de acceso aleatorio	Memoria USB (universal serial bus)	Memoria SD
Memoria Micro SD	Alm. óptico de datos (CD-DVD)	Equipos terminales móviles	Tabletas electrónicas
Modulador (Modem)	Enrutadores (Router)	Equipos Sistema de Posicionamiento Global (GPS)	Otros dispositivos electrónicos que almacenen información
Tarjetas SIM Card			

1.2 Identificación de riesgos

Evidencia digital o información almacenada electrónicamente:

	Físico	Lógico
Evidencia digital	Destrucción parcial o total de la fuente de almacenamiento de información.	Manipulación de registros.
Información almacenada electrónicamente	Caídas, movimientos bruscos, golpes, fricción con un campo magnético (Energía, 2014), exposición a radiaciones electromagnéticas (Radiación electromagnética, s. f.) del dispositivo tecnológico donde se encuentre contenida la evidencia digital.	Pérdida de autenticidad por el tratamiento directo de datos. Modificación de su huella digital.

1.3 Prevención del riesgo:

Una buena práctica para prevenir el riesgo de contaminación de cualquier dispositivo electrónico, es tener en cuenta que, al momento de trabajar con la evidencia digital, se debe implementar y utilizar los elementos de bioseguridad (tapa bocas, guantes

antiestáticos, bata antiestática, manilla antiestática, gafas de protección), como una medida que garantice y minimice los impactos negativos sobre el dispositivo objeto de la recolección.

Fig. 1. Elementos de bioseguridad

Es recomendable que el practicante cuente con las mínimas medidas de seguridad al momento de hallar cualquier evidencia digital o información electrónicamente almacenada, previniendo que en lo posible no tenga contacto con campos electromagnéticos de frecuencias altas que se encuentren cerca, como también es recomendable que el practicante se despoje de elementos conductores de energía que tenga puestos en su cuerpo.

Para aclaración del practicante, las fuentes de campo electromagnético según la Organización Mundial de la Salud, manifiestan que; "*Cualquier conductor eléctrico cargado genera un campo eléctrico asociado, que está presente, aunque no fluya la corriente eléctrica. Cuanto mayor sea la tensión, más intenso será el campo eléctrico a una determinada distancia del conductor*" (Salud, s.f.).

Los campos electromagnéticos de frecuencias altas, se pueden encontrar en teléfonos móviles, televisores y trasmisores de radio (Salud, s.f.), por lo anterior y en vista de los diferentes entornos en que se puede hallar una evidencia digital, el practicante debe prevenir que el aparato electrónico o cualquier dispositivo en su momento, deba ser apartado de estos factores que pueden interferir de manera indirecta al procedimiento de preservación y embalaje del elemento material de prueba o evidencia física.

Ahora bien, la electricidad estática que produce la especie humana, se exterioriza en condiciones secas, por consiguiente, se recomienda como buena práctica, antes de manipular cualquier aparato electrónico o circuito, tocar alguna superficie metálica o una pared, con la finalidad de poder descargar eléctricamente el cuerpo o si entre sus posibilidades cuenta con una pulsera antiestática (StartTech.com, s.f.) puede utilizarla. Esto prevé que al momento de tocar cualquier dispositivo electrónico pueda presentarse daños microscópicos que lleguen a ser la causa de la pérdida demostrativa en un estrado judicial.

Fig. 2. Pulsera antiestática

La manipulación inadecuada del dispositivo puede ocasionar daños físicos del elemento material probatorio o evidencia física, tal como lo son; impactos, caídas, maniobras bruscas del elemento o ser expuesta a sustancias, fluidos o variación en temperatura ambiente.

1.4 Procedimiento cuando se halla un dispositivo electrónico encendido

Como primera medida se debe de identificar el tipo de dispositivo electrónico, seguidamente se deberá de proceder de acuerdo a la clasificación del elemento hallado de la siguiente manera:

Para equipos y terminales móviles con sistemas operativos Android encendidos, como buena práctica se debe realizar una inspección visual sobre el dispositivo (uso de elementos de bioseguridad), verificando si el dispositivo se encuentra protegido con algún sistema de seguridad para la autenticación de usuario (patrones de bloqueo, pin de seguridad o clave personalizada), se debe realizar la fijación fotográfica y documentación del estado en el cual fue hallado, posteriormente se debe recolectar y embalar sin ser manipulado ni apagado (dejar que se descargue en su totalidad) con la finalidad de asegurar la integridad del dispositivo físico para análisis de laboratorio.

Para computadoras de escritorio encendidas, como buena práctica se debe realizar una inspección visual sobre el dispositivo (uso de elementos de bioseguridad), verificando si el dispositivo se encuentra protegido con algún sistema de seguridad para la autenticación de usuario, seguidamente se debe de realizar la fijación fotográfica y documentación del estado en el cual fue hallado, se continua desconectando el cable de poder que suministra la energía a la máquina del toma corriente, no debe de ser apagado manualmente. Como recomendación, no extraer el dispositivo de almacenamiento sino cuenta con los conocimientos adecuados o instrumentos requeridos, es recomendable enviar la torre del computador como fue hallada para su respectivo peritaje. Ahora bien, si el dispositivo se encuentra sin ninguna seguridad, es importante realizar adquisición de data volátil para preservar la información cargada en memoria principal.

Para computadoras portátiles encendidas, como buena práctica se debe realizar una inspección visual sobre el dispositivo (uso de elementos de bioseguridad), verificando si el dispositivo se encuentra protegido con algún sistema de seguridad para la autenticación de usuario, seguidamente se debe realizar la fijación fotográfica y documentación del estado en el cual fue hallado, pero si el dispositivo se encuentra sin ninguna seguridad, es importante realizar adquisición de data volátil para preservar la información cargada en memoria principal (es recomendable contar con el cargador de batería). Para los dos casos mencionados no se deberá apagar la máquina, se recolecta y embala el dispositivo permitiendo que se descargue en su totalidad.

Reloj *Smart,* se deberá realizar una inspección visual sobre el dispositivo (uso de elementos de bioseguridad), seguidamente se debe de realizar la fijación fotográfica y documentación del estado en el cual fue hallado, para mitigar el riesgo de la manipulación se debe recolectar y embalar de manera inmediata para ser analizado por parte del laboratorio, es recomendable no apagar ni generar ningún registro de eventos por movimientos de los aplicativos internos del sistema.

En caso de hallar otros dispositivos, se recomienda no apagar de manera manual, dejar descargar la batería en su totalidad, procediendo a recolectar y embalar.

1.5 Nivel de madurez en una evidencia digital

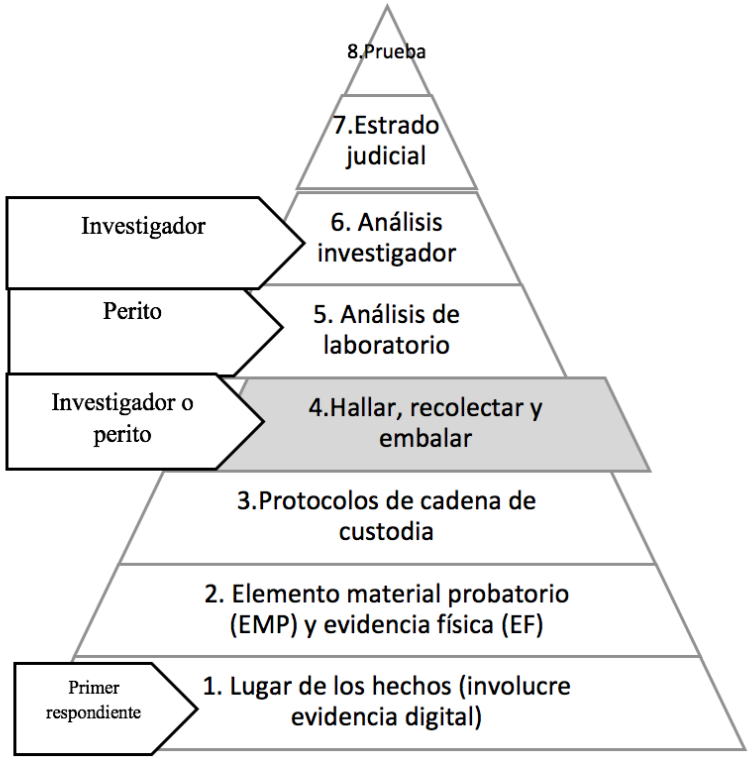


Fig. 3. Nivel de maduración de una evidencia digital

El procesamiento de evidencia digital como metodología en el tratamiento y análisis del EMP y EF, auxilia al desarrollo teórico-práctico de la actividad forense, contribuyendo en gran medida al trabajo investigativo por parte del ente involucrado o las partes interesadas. Ahora bien, la implementación práctica de cada etapa; identificación, recolección, preservación, análisis y entrega de resultados, pretende aumentar el nivel de madurez de la evidencia, sin embargo, otras variables son sumadas; las condiciones en que fue encontrado y los indicadores de compromiso, para finalmente asociar la evidencia con el ejecutor del hecho. Si el dictamen técnico pericial entregado, producto del análisis, es validado ante un estrado judicial, se da por hecho que en razón al mismo se considera una prueba que pretende mostrar y hacer patente la verdad o falsedad de algo en específico.

La prueba contundente dentro de una investigación, está sujeta al cumplimiento de una serie de buenas prácticas en cada una de sus etapas, desde el momento en que se genera un hecho de naturaleza delictiva, como el hallazgo de evidencia digital con posibilidad de llegar a ser una prueba, hasta la utilización de los protocolos de cadena de custodia para la recolección y el embalaje, deben cumplir con las mínimas medidas de seguridad para la prevención del riesgo. Dentro de la etapa (4) donde se debe preservar la integridad de la evidencia, es necesario aplicar la metodología propuesta, la cual busca asegurar la continuidad de la cadena de custodia hasta el punto de alcanzar el grado de madurez dentro del proceso investigativo.

Es necesario que el ejecutante documente la actividad realizada, iniciando por el hallazgo, la recolección y el embalaje, así mismo detallar en qué condiciones se encuentra el elemento, cual fue la metodología para el tratamiento, como también cuales fueron los procedimientos implementados y por último las observaciones como profesional.

1.6 Análisis

	Evidencias procesadas		
	2017	2018	
DIJIN	245	178	423
MEBOG	213	229	442
Regional 2	84	90	174
Regional 3	209	229	438
Regional 4	105	99	204
Regional 5	197	130	327
Regional 6	597	729	1.326
Regional 7	91	67	158
Regional 8	135	91	226
Total	1876	1842	3718

Fig. 4. Número de casos que involucra evidencia digital

A. Contextualización

Tomando a modo de referencia los diferentes Laboratorios de Informática Forense que componen la Dirección de Investigación Criminal e Interpol de la Policía Nacional de Colombia (Centro Cibernético Policial de Colombia, 2017), para los años 2017-2018 fueron procesadas 3.718 evidencias, inmersas en procedimientos judiciales, por delitos de: homicidios, hurtos, estupefacientes, amenazas y rebelión, así mismo se desprenden modalidades propias al delito informático como uso de *software* malicioso, injuria, violación de datos personales, suplantación de sitios web, captura de datos personales, pornografía con personas menores de edad, injuria y/o calumnia, suplantación de identidad, estafa por compras online, *phishing*, *vishing*, *malware, ransomware,* carta nigeriana y amenazas a través de medios informáticos.

Cabe resaltar que, de la totalidad de evidencias procesadas, un 70% son solicitudes de análisis a dispositivos electrónicos de naturaleza digital, por tanto, es conveniente resguardar los procedimientos mediante buenas prácticas dentro del procesamiento de evidencia; sobre todo si el elemento es sensible a cambio.

2. Método

En la búsqueda de un proceso investigativo legítimo, donde la evidencia no llegue a ser alterada, es necesario implementar un método de recolección dentro del procesamiento de evidencia digital, el cual apoye la tarea del investigador y mantenga integro el elemento. Para lo cual se plantea una solución óptima y necesaria, que en principio proteja físicamente la evidencia de cualquier factor externo, como también mantenga los principios de cadena de custodia, la cual se plantea a continuación:

El material a utilizar para la construcción de contenedores para el almacenamiento de la evidencia, debe de ser aislante de campos eléctricos y campos magnéticos, toda vez que se requiere que la preservación del elemento no llegue a ser contaminada con partículas que degraden las características particulares del mismo.

A continuación, se mencionan algunos materiales que desde el punto de vista generalizado de la actividad del perito informático y reglas de la sana crítica se consideran que son necesarios al momento de elaborar contenedores para el embalaje de evidencia digital o información almacenada electrónicamente, en caso de no contar con bolsas antiestáticas y de ser necesario la inmediatez del procedimiento de recolección, se puede utilizar:

Papel aluminio, que funciona como repelente de radiaciones electromagnéticas y a su vez genera una Jaula de Faraday (Juliana, 2013) convencional para la anulación del efecto en campos externos y generando una polarización del conductor de carga eléctrica, al ser una fina capa de aluminio cuenta con dos lados diferentes, uno más brillante que otro, esto se debe a que tienen una funcionalidad particular; cuando se piensa embalar un dispositivo electrónico se debe utilizar el lado más brillante hacia afuera y el lado opaca hacia adentro, debido a que la cara opaca se encarga de absorber las temperaturas exteriores y su lado contrario se encarga de repeler las señales electromagnéticas externas.

Poliestireno, conocido en el mercado como icopor, se puede utilizar para la elaboración del contenedor por su resistencia a la humedad y capacidad de absorción de impactos (EPS Molders Association, 2012), por lo cual lo hace idóneo para ser implementado.

Cartón ondulado o corrugado (Zuleta, 2013), este material es resistente al apilamiento, así mismo cumple la función de aislar el elemento de los diferentes factores ambientales externos que pueden ser causal de diferentes riesgos.

Cinta aislante, preferiblemente de color rojo, para identificar la alimentación de circuitos PCB (Torres-Ortega, 2014).

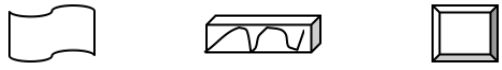
2.1 Elaboración de un contenedor y embalaje de la evidencia digital

Seguidamente se muestran los pasos a seguir para la elaboración práctica de un contenedor que en su interior aísle un dispositivo electrónico, para mitigar riesgos como: radiaciones electromagnéticas, impactos o caídas y factores ambientales que representen una amenaza a la evidencia, a su vez se recomienda disponer de un lugar en óptimas condiciones de aseo para el procedimiento de embalaje.

1. Conocer las dimensiones: cm (ancho) x cm (largo) x cm (alto), de la evidencia objeto de embalaje.

Fig. 5. Aparatos o dispositivos electrónicos

2. Tener listos los materiales.



3. Contar con los elementos de bioseguridad e implementarlos al momento de realizar la práctica.

4. **Paso 1.** Cortar el papel aluminio con las medidas extraídas del numeral uno.

5. **Paso 2.** Cortar el icopor de (1cm.) al tamaño indicado del numeral uno.

6. **Paso 3.** Cortar el cartón ondulado o corrugado con las medidas establecidas sumando un centímetro a su dimensión.

7. **Paso 4.** Constatar que la evidencia de naturaleza electrónica se encuentre apagada o desconectada de su fuente de energía, cubriendo con cinta aislante la alimentación de los circuitos PCB ("*Printed Circuit Board*") placa de circuitos impresos.

8. **Paso 5.** Observar que la evidencia no se encuentre húmeda o contenga alguna clase de material que pueda oxidar alguna parte electrónica del dispositivo.

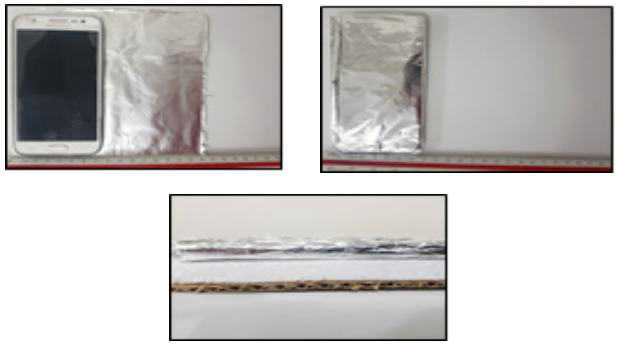
9. **Paso 6.** Utilizando el recorte de papel aluminio, se procede a cubrir en su totalidad la evidencia. Recordar que el lado más brillante debe ir hacia afuera.

10. **Paso 7.** Una vez cubierta la evidencia con el papel aluminio se procede a cubrir con el icopor.

11. **Paso 8.** Se procede a cubrir en su totalidad la evidencia con el cartón corrugado y como sellante se debe utilizar cinta transparente.

12. **Paso 9.** Verificar que la cubierta del contenedor este sellada y no haya rupturas ni espacios sin cubrir.

13. **Paso 10.** Por último y no menos importante, se debe utilizar el protocolo de cadena de custodia, como mecanismo de autenticación y validación ante cualquier estrado judicial.



Fotografías de materiales, fuente propia.

3. Resultados

Como resultado se expone una metodología adecuada, bajo un patrón de diseño de buenas prácticas, dirigido al investigador o perito informático, para la elaboración de contenedores que sirvan para el debido embalaje de evidencia digital o información almacenada electrónicamente en un escenario criminal, para ser objeto de análisis y posteriormente ser sometido a procedimientos judiciales.

En la actualidad se cuenta con diferentes artículos investigativos en los principales motores de búsqueda en internet sobre la identificación de la evidencia digital y al manejo de la misma, definiendo los conceptos en ámbito forense, y que a su vez enriquece el conocimiento del experto, pero no se contaba con una metodología de buenas prácticas con relación a la elaboración de contenedores para el embalaje de evidencia digital, debido a que no en todos los escenarios criminales se cuenta con bolsas antiestáticas de fabricación en serie.

4. Discusión

Diferentes métodos y materiales existen en el medio para poder realizar el procedimiento de embalaje, pero el objetivo de este artículo es mostrar la manera más adecuada para no ir a incurrir en fallas humanas que puedan distorsionar o dilatar el procedimiento investigativo por el desconocimiento de buenas prácticas a la hora de la recolección de evidencia digital.

5. Conclusión

La informática forense avanza a gran escala, a causa de la mutación del accionar delincuencial y criminal, por lo cual el investigador y perito, debe estar en capacidad de afrontar cualquier escenario criminal y una de las maneras en que pueda lograrlo es mediante buenas prácticas en los procedimientos que realice, más en el tema de preservación y recolección de evidencia, por tal razón y en conclusión es necesario aprender a utilizar los recursos necesarios con los que se cuenten y que

estos sean de fácil acceso utilizando buenas prácticas para no incurrir en errores y sean válidos en cualquier estrado judicial.

6. Agradecimientos

A Dios, Familia y al Centro Cibernético Policial de la Dirección de Investigación Criminal e Interpol Policía Nacional de Colombia.

Referencias

Centro cibernetico policial de Colombia. (2017). *Informe amenazas de cibercrimen en colombia 2016 - 2017*. https://caivirtual.policia.gov.co/contenido/informe-amenazas-del-cibercrimen-en-colombia-2016-2017

Congreso de la República (2004). Ley 906 de 2004, Por la cual se expide el Código de Procedimiento Penal. (Corregida de conformidad con el Decreto 2770 de 2004). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=14787

Icontec. (2013). Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos Ntc-Iso/Iec 27001. Icontec, 37.

Energía. (17 de febrero de 2014). *Britannica Digital Learning.* https://britannica.es/

EPS Molders Association. (2012). *EPS History.* **http://www.epsmolders.org**

Fiscalía General de la Nación (2016). Resolución 02369 del 2016, Por medio de la cual se adopta el Manual de procedimientos para cadena de custodia y se deroga la Resolución 0-1874 de 21 de junio de 2016. https://normativa.colpensiones.gov.co/colpens/docs/resolucion_fiscalia_2369_2016.htm

Juliana, E. (2013). La jaula de Faraday. *La Vanguardia.* https://www.lavanguardia.com/opinion/articulos/20130312/54369198420/la-jaula-de-faraday-enric-juliana.html

Organizacion Mundial de la Salud. (s.f.). Salud. https://www.who.int/es

Pollitt, M. M. (2001). *Report on digital evidence.* 13th Interpol Forensic Science Symposium.

Radiación electromagnética (s.f.). Google Libros.

Rosado, F. R. (2011). La informática forense: el rastro digital del crimen. *Derecho y Cambio Social, 8*(25), 9. https://dialnet.unirioja.es/servlet/articulo?codigo=5497990

StartTech.com (s.f.). Pulsera antiestática con cable a tierra - brazalete. https://www.startech.com/media/products/SWS100/PDFs/SWS100_Datasheet-ES.pdf

Torres-Ortega, H. (2014). *Guía de diseño PCB con Eagle.* Guadalajara: Herramientas Tecnológicas Profesionales. https://hetprostore.com/images/Tutoriales/pcb_eagle/hetpro_tutorial_pcb_eagle.pdf

Withers, K. J. (s.f.). Información almacenada electrónicamente: Las enmiendas de diciembre de 2006 a las reglas federales de Procedimiento Civil. *Diario noroeste de tecnología y propiedad intelectual, 4*(2), 171.

Zuleta, A. (2007). *Manual de elaboración del cartón ondulado. ASIGMA S.L*, 158.