ESTUDIO DE VULNERABILIDADES EN EL PROCESO DE CADENA DE CUSTODIA DE EVIDENCIAS EN DELITOS INFORMÁTICOS EN LA CIUDAD DE CARTAGENA

RAMÓN ANDRÉS PATERNINA CUESTA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELADE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
ESPECIALIZACION EN SEGURIDAD INFORMATICA
CARTAGENA
2018

ESTUDIO DE VULNERABILIDADES EN EL PROCESO DE CADENA DE CUSTODIA DE EVIDENCIAS EN DELITOS INFORMÁTICOS EN LA CIUDAD DE CARTAGENA

RAMÓN ANDRÉS PATERNINA CUESTA

Proyecto Aplicado – Informática Forense

Director de proyecto
Ing. Jorge Enrique Ramírez Montanez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELADE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
ESPECIALIZACION EN SEGURIDAD INFORMATICA
CARTAGENA
2018

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Cartagena de Indias 19 de Septiembre 2018

DEDICATORIA:

A mis padres, Amira Cuesta Orosco y Ramón Paternina Bru, siendo ellos los motivadores para emprender este camino de fortalecimiento en el desarrollo de mi vida profesional.

AGRADEZCO A:

Primeramente a Dios por siempre estar presente y llenarme de su inmensa misericordia.

A mi esposa por ser ese pilar que siempre estuvo sosteniéndome y motivándome, en los momentos de angustia, de estrés, siempre brindando su amor y apoyo incondicional.

A mi Hermano Juan por sus consejos y apoyo.

A mi director de proyecto el Ingeniero Jorge Enrique Ramírez Montanez por su paciencia, dedicación y constante seguimiento en el desarrollo del proyecto.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pag.

LISTA DE ANEXOS

Pág.

TITULO

ESTUDIO DE VULNERABILIDADES EN EL PROCESO DE CADENA DE CUSTODIA DE EVIDENCIAS EN DELITOS INFORMÁTICOS EN LA CIUDAD DE CARTAGENA

INTRODUCCION

La seguridad informática es la disciplina que determina los procesos, protocolos o métodos que permiten establecer condiciones seguras para el manejo de la información y elementos de un sistema informático, garantizando la confidencialidad, integridad y disponibilidad de los mismos.

La seguridad informática es algo que se aplica de manera transversal en los diferentes ámbitos en los cuales un dato, una información o un elemento grafico se constituyen en una pieza indispensable para el esclarecimiento de una situación determinada, como en el caso al cual hace referencia el presente trabajo, que se refiere al proceso de cadena de custodia en los delitos informáticos, teniendo en cuenta que de la seguridad del protocolo utilizado para sustraer, proteger y validar evidencias, depende la efectividad que estas puedan tener como elementos probatorios en la investigación de un delito informático.

Se busca mediante un estudio descriptivo identificar que vulnerabilidades se pueden presentar o si se están presentando en los procesos de cadena de custodia que se realizan en los casos pertenecientes a delitos informáticos que se llevan a cabo en la ciudad de Cartagena. Se revisarán diversas fuentes de información donde se describan las diferentes prácticas que se deban llevar a cabo durante un proceso de cadena de custodia, específicamente sobre evidencia digital y de igual manera sobre evidencia física que está inmersa la ejecución del delito informático y se dispongan como elementos materia de prueba.

De igual manera se realizarán una entrevista con personal del cuerpo técnico de investigación de la Fiscalía General de la Nación Seccional Bolívar más específicamente a unidad de delitos informáticos para indagar sobre los procedimientos de cadena de custodia y el manejo de evidencia digital en los delitos informáticos en la ciudad de Cartagena.

Lugo de finalizar el estudio se adoptan una serie de controles según la norma ISO 27002, para la mitigación de los riesgos encontrados, posteriormente se detallan unas recomendaciones para el trato de la evidencia digital en el proceso de cadena de custodia, con el fin de que estas no pierdan su valor probatorio, debido a una mala manipulación de las mismas.

1. DESCRIPCION DEL PROBLEMA

La cadena de custodia informático – forense tiene como finalidad brindar soporte veraz a la pruebas digital, por tal motivo, el procedimiento que es realizado en la ciudad de Cartagena para la sustracción de la evidencia informática, desde su localización hasta su valoración, debe garantizar que no existan suplantaciones, modificaciones, alteraciones, adulteración o destrucción de los indicios materiales relacionados con un hecho delictivo, que conlleve a la posible impugnación de la evidencia debido a errores metodológicos en el procedimiento empleado para su obtención y resguardo.

La maleabilidad de la evidencia digital, su facilidad para ser duplicada e igualmente modificable es lo que la hace vulnerable a que pierda su valor probatorio.

1.1 FORMULACION DEL PROBLEMA

¿Cómo la identificación de factores que pueden afectar la evidencia en el proceso de cadena de custodia en delitos informáticos, permitirá brindar un soporte eficiente al manejo de pruebas digitales, con el fin de preservar la integridad, confidencialidad y disponibilidad de la evidencia como elemento probatorio en los procesos judiciales en la ciudad de Cartagena?

2. JUSTIFICACION

La cadena de custodia, es un procedimiento de control que se ejerce sobre los elementos materiales probatorios y evidencia física relacionados con el delito. Tiene inicio desde las vulnerabilidades identificadas en el proceso de cadena de custodia de evidencias en delitos informáticos. Sobre las vulnerabilidades identificadas en el proceso de cadena de custodia de evidencias en delitos informáticos.

En la Investigación Judicial, debe garantizarse en todo momento la validez de las posibles evidencias, a fin de evitar la pérdida de la efectividad que estas puedan tener como elementos probatorios en la investigación de un delito.

La inspección que se hace en el escenario del delito, tiene por objeto determinar qué sucedió allí, por lo que el éxito de la reconstrucción y validez de los resultados, depende, de que el procedimiento se ajuste totalmente a las exigencias legales y técnicas establecidas.

Además, si se tiene en cuenta que a pesar del rigor en la obtención de la evidencia, existe la presunción de resultados probables y por lo tanto no infalibles o absolutamente ciertos, con mayor razón surge la necesidad de introducir todas las garantías procesales posibles para lograr una mayor fiabilidad en las conclusiones derivadas del análisis de los materiales probatorios, es decir, es indispensable un estricto apego a los procedimientos legales y científicos, y es precisamente allí donde se encuentra la razón de ser del concepto jurídico que se denomina Cadena de Custodia de la Evidencia.

La importancia de la investigación sobre la cadena de custodia radica en la posibilidad de identificar factores, elementos o situaciones que debilitan el proceso, conllevando a que se vicie la evidencia mediante acciones que modifiquen su contenido o significado, impidiendo que cuente con la autenticidad y fiabilidad que garanticen su validez para

ser utilizada por la autoridad competente a fin de analizar y obtener, por parte de los expertos, técnicos o científicos un concepto pericial.

Lo anterior beneficia en diferentes instancias a los vinculados de manera directa o indirecta a una investigación, pues contar con una herramienta como el informe que resultará de la presente investigación, coadyuva a generar seguridad sobre la validez de la evidencia, en el sentido de haber identificado y subsanado oportunamente posibles vulnerabilidades en el proceso de la cadena de custodia de las evidencias.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar un estudio de vulnerabilidades en el proceso de cadena de custodia con el fin de brindar un soporte eficiente al manejo de las pruebas digitales, identificando factores que pueden afectar la evidencia en el proceso de cadena de custodia, en delitos informáticos en la ciudad de Cartagena

3.2 OBJETIVOS ESPECIFICOS

- Recolectar información acerca del proceso de cadena de custodia de la evidencia digital en delitos informáticos, mediante métodos de investigación, para recolección y custodia de la evidencia, como posible elemento probatorio

- Comparar los procedimientos establecidos en los protocolos actuales del proceso de cadena de custodia, utilizados por el área de Delitos Informáticos de la Fiscalía Seccional Cartagena, frente a las normas y estándares establecidos para el manejo de la evidencia digital para detectar inconsistencias o falencias en el procedimiento realizado.

- Presentar resultados del estudio, controles según la norma ISO 27002 y una serie de recomendaciones pertinentes para las distintas fases del proceso de cadena de custodia en cuanto al manejo de las evidencias digitales

4. MARCO REFERENCIAL

4.1 ANTECEDENTES

Con la entrada en vigencia del Sistema Acusatorio Penal, surgieron nuevas obligaciones para las autoridades colombianas, en este proceso el papel de la Fiscalía General de la Nación y de los Organismos de Policía Judicial en materia de investigación criminal se hizo más exigentes en cuanto al manejo de la investigación y los elementos que puedan servir de prueba en el juicio.

Colombia fue el primer país en crear un Manual de procedimiento de cadena de custodia, mediante la Resolución 0-6394/ 2004, redactado por la Fiscalía General de la Nación. Este manual da un tratamiento detallado para cada elemento de prueba por separado y marca sus fundamentos en los artículos 67, 114, 208, 213, 214, 215, 216, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 268, 276, 277, 278, 279, 280, 281, 484, 485, todos de la Ley 906 de 2004 (Código de Procedimiento Penal). El mismo regula por separado las distintas fases de la cadena de custodia y va dirigido a los servidores públicos y personal que tenga acceso a cualquier elemento de prueba de una proceso penal. [1]

En el año 2009 se crea en Colombia la ley 1273, Por medio de 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"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones; esta ley tipifica las diferentes acciones que constituyen delitos informáticos, esta situación supone el planteamiento de múltiples interrogantes frente a la eficacia de los procedimientos para el proceso de cadena de custodia de

[1]FISCALIA GENERAL DE LA NACION. MANUAL DE PROCEDIMIENTOS PARA CADENA DE CUSTODIA. [En Línea] Bogotá "Enero de 2012". [Citado en 23 Marzo de 2016], Disponible en Internet: < http://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/01/manualcadena2.pdf>

las evidencias recolectadas como posible material probatorio en la investigación de estos delitos informáticos.

Realizada una búsqueda vía web se pueden referenciar proyectos investigativos sobre la temática abordada por la presente propuesta:

- Propuesta de un modelo de procedimiento para el tratamiento de la evidencia digital, acorde a la normatividad colombiana sobre delitos informáticos. Orientado a formular un Procedimiento y una Guía con el fin de mejorar el tratamiento de la evidencia digital como medio técnico de soporte judicial, mediante la aplicación de mecanismos forenses, dirigido apersonas que desarrollan funciones y tareas de Investigación judicial desde el campo Técnico – Científico. [2]
- La cadena de custodia en el sistema penal acusatorio**.**[3]
- Cadena de custodia, su trascendencia y aplicación en sistema penal acusatorio durante 2005-2006. Busca proporcionar una herramienta de consulta a estudiantes de derecho y de otras facultades, lo mismo que a personal de policía judicial de los diferentes organismos seguridad (DAS, SIJIN DIJIN, CTI), médicos y paramédicos de centros hospitalarios, clínicas, Medicina legal, y otras autoridades competentes como responsables de la recolección y manejo de las evidencias físicas, que permita estandarizar un manejo adecuado y eficaz de las elementos materiales probatorios correspondientes a una investigación penal y que posteriormente se convertirán en pruebas, en su debido momento, esto es, el juicio oral. [4]

---

[2] GAVIRIA, Pablo. PROPUESTA DE UN MODELO DE PROCEDIMIENTO PARA EL TRATAMIENTO DE LA EVIDENCIA DIGITAL, ACORDE A LA NORMATIVIDAD COLOMBIANA SOBRE DELITOS INFORMÁTICOS. [En Línea] Pasto “Enero 10 de 2015” [Citado en 26 Abril de 2016], Disponible en internet: < http://hdl.handle.net/10596/4008>

[3] HENAO NOREÑA, Juan. LA CADENA DE CUSTODIA EN EL SISTEMA PENAL ACUSATORIO [En línea], Medellín “2012”. [Citado en 23 Marzo de 2016], Disponible en internet: <http://repository.udem.edu.co/bitstream/handle/11407/277/La%20cadena%20de%20custodia%20en%20el%20Sistema%20Penal%20Acusatorio.pdf?sequence=1>

[4] ARBOLEDA MURRILLO, Henry, et al. CADENA DE CUSTODIA, SU TRASCENDENCIA Y APLICACION EN SISTEMA PENAL ACUSATORIO DURANTE 2005-2006 [En Línea], Manizales “2007”. [Citado en 23 Marzo de 2016], Disponible en Internet:<http://ridum.umanizales.edu.co:8080/xmlui/bitstream/handle/6789/523/140_Murillo_Arboleda_Henry_2007.pdf?sequence=1>

- Procedimientos en la investigación, recolección y manejo de la evidencia digital en la escena del crimen. dar a conocer y establecer los procedimientos en la investigación y manejo de la evidencia digital, con el fin de establecer lineamientos a seguir cuando éstos sean requeridos para efectuar una investigación objetiva, clara y precisa y de esta manera obtener los resultados deseados para poder aportar con claridad y precisión indicios que orienten las decisiones en casos donde se requiera.[5]

4.2 MARCO TEÓRICO

4.2.1 Informática Forense. La informática forense es una disciplina que se dedica a la recolección de evidencias o pruebas de carácter digital empleando técnicas de análisis e investigación para que posteriormente puedan ser usadas con fines judiciales.

El tipo de pruebas digitales obtenidas a partir de un examen forense que se realiza en una máquina computacional puede ser útil en una amplia gama de investigaciones judiciales como por ejemplo:

• Litigios civiles en los casos de divorcio y el acoso.
• Evidencia de malversación de fondos, fraude o robo sobre propiedad intelectual.
• Pruebas en la discriminación por edad, sexo, raza o por despido injustificado
• Investigaciones de compañías de seguros cuando se exijan pruebas relativas al seguro
• Fraude, homicidio culposo
• Casos relacionados con seguros y reclamaciones

[5] SANTOS TELLO, Jorge. PROCEDIMIENTOS EN LA INVESTIGACIÓN, RECOLECCIÓN Y MANEJO DE LA EVIDENCIA DIGITAL EN LA ESCENA DEL CRIMEN. [En linea] Hueheutango "Septiembre de 2013". [Citado en 28 Marzo 2016], Disponible en internet: < http://biblio3.url.edu.gt/Tesario/2013/07/03/Santos-Jorge.pdf>

• Se utiliza en la recuperación de información que haya sido borrada, cifrado dañado.

La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.[6]

4.2.2 Delitos Informáticos. Son todos aquellos actos o conductas ilícitas, dirigidas a alterar o destruir cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión.

4.2.3 Clasificaciones del delito informático. Los delitos informáticos se pueden clasificar en los siguientes grupos de delitos:

• Fraudes cometidos mediante manipulación de computadores. Se refiere a la manipulación de datos o de programas, ya sea colocando datos falsos en un sistema u obteniendo los datos del sistema de manera ilegal

• Falsificaciones Informáticas. En este punto se trata de falsificación de dineros, cuentas Bancarias, entre otros, mediante la utilización de equipos de cómputo.

• Daños a Datos Computarizados. Se trata de la realización de acciones dañinas para un sistema, tales como accesos no autorizados, empleo de virus o gusanos.

El delito informático está ligado a la informática y a todo bien jurídico que esta implica, como lo son: datos, programas, documentos electrónicos, dinero electrónico e información.

Entre los delitos informáticos que se presentan con mayor frecuencia están:

• *Hacking*. Se denomina "*hacking*" en la jerga informática a la conducta de entrar a un sistema de información sin autorización, es decir violando las barreras de protección establecidas a tal fin. El sujeto que realiza esta actividad es llamado hackers, muy rara vez se conoce su nombre verdadero y en mucho casos actúa y firma en grupo. La actividad de hackear un sistema puede tener diferentes

---

6 UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD. [En Linea] (s.f.). [Citado en 23 de Marzo de 2016], Disponible en internet:< http://campus03.unad.edu.co/ecbti04/mod/lesson/view.php?id=10442>

finalidades y alcances. Así, en la mayoría de los casos el romper el sistema o eliminar los pasos de seguridad de un sistema tiene por objeto ver, fisgonear el contenido y la información protegida o extraer copias de la información o destruirla.7

- *Cracking*. Se conoce como *cracking* la acción de cambiar los contenidos de la información; procedimiento orientado a destruir el sistema; a las personas que se dedican a realizar esta actividad se les identifica como *crackers*.
- Lo que caracteriza esta conducta delictiva, es la entrada ilegal al sistema, es decir, que la persona no cuenta con los *password* o no los ha conseguido adecuadamente.
- *Phreaking*. Es la actividad de utilizar líneas telefónicas, encontrando la forma de evitar pagar por el uso de la red telefónica ya sea pública o privada, digital o inalámbrica.
- El *phreaking* es, por lo general, la más común de las conocidas como actividades informáticas ilícitas.
- *Carding*. Se llama *Carding* al hecho de cometer un fraude o una estafa con un número de tarjeta de crédito u otras que tienen la capacidad de recargarse.
- Para que el fraude con tarjeta de crédito se transforme en *Carding*, debe haberse usado un número de tarjeta de crédito ya sea, de una existente o de una creada mediante procedimientos digitales para realizar compras por Internet o efectuar pagos.

[7] SANTOS TELLO, Jorge. PROCEDIMIENTOS EN LA INVESTIGACIÓN, RECOLECCIÓN Y MANEJO DE LA EVIDENCIA DIGITAL EN LA ESCENA DEL CRIMEN. [En linea] Hueheutango “Septiembre de 2013”. [Citado en 28 Marzo 2016], Disponible en internet: < http://biblio3.url.edu.gt/Tesario/2013/07/03/Santos-Jorge.pdf>

4.2.4 Cadena de Custodia. Es el procedimiento que busca evitar alteraciones o modificaciones, en los elementos materiales relacionados con un hecho delictivo, con el fin de salvaguardar su efectividad al momento de ser utilizado como evidencia en la investigación de un delito.

Teniendo en cuenta lo anterior, en estos casos se debe aplicar un riguroso procedimiento técnico a los elementos, desde que se tomaron hasta su almacenamiento.

Estas medidas restringirán el acceso a la evidencia, permitiendo identificar responsabilidades ante manipulaciones incorrectas o intentos de acceso no autorizados.

Revisando el manual para el manejo de evidencias digitales y entornos informáticos creado por el Dr. Santiago Acurio del Pino como una guía de actuación para miembros de la Policía Judicial así como de los Funcionarios de la Fiscalía, cuando en una escena del delito se encuentren dispositivos Informáticos o electrónicos que estén relacionados con el cometimiento de una infracción de acción pública.

En dicha guía el Dr. Santiago da algunas recomendaciones al momento de realizar ya sea un allanamiento o incautación de equipo informáticos, que son[8]:

1. ¿A qué horas debe realizarse?

- Para minimizar destrucción de equipos o datos
- Muy probablemente sospechoso tal vez estará en línea
- Seguridad de los investigadores o personas encargadas de las mismas.

2. Entrar sin previo aviso

- Evitar destrucción y alteración de los equipos o la evidencia contenida en esta.

[8] ACURIO DEL PINO, Santiago. MANUAL DE MANEJO DE EVIDENCIAS DIGITALES Y ENTORNOS INFORMÁTICOS. [En Linea] "07 de Julio de 2009". [Citado en 20 de Octubre de 2016], Disponible en internet:<http://www.oas.org/juridico/english/cyb_pan_manual.pdf>

El siguiente punto hace énfasis en los materiales para poder llevar a cabo una buena cadena de custodia,

3. Materiales previamente preparados

- Embalajes de papel
- Etiquetas
- Discos y disquetes vacíos
- Herramienta protectora de escritura (discos duros)
- Cámara fotográfica

4. Realizar simultáneamente los allanamientos e incautación en diferentes sitios

- Datos pueden estar en más de un lugar, sistemas de red, conexiones remotas.

5. Examen de equipos

6. Aparatos no especificados en la orden de allanamiento

7. Creación de Respaldos en el lugar, creación de imágenes de datos.

- Autorización para duplicar, reproducir datos encontrados (por ejemplo, un aparato contestador)

8. Fijar/grabar la escena

- Cámaras, videos, etiquetas

9. Códigos/claves de acceso/contraseñas

10. Buscar documentos que contienen información de acceso, conexiones en redes, etc. [9]

[9] Ibíd. , p. 24

4.3 MARCO CONCEPTUAL

• Elemento Materia de prueba ‘EMP’ o Evidencia Física ‘EF’**:** Elementos físicos que se recaudan por un investigador como consecuencia de un acto delictivo, los cuales pueden servir en la etapa del juicio para demostrar que la teoría del caso que se expone ante el juez es cierta y verificable.

Elementos relacionados con una conducta punible que sirven para determinar la verdad en una actuación penal.[10]

• Evidencia Física**:** Todo elemento tangible que permite objetivar una observación y es útil para apoyar o confrontar una hipótesis.[11]

• Impunidad**:** Falta de castigo, esto es, libertad de que un delincuente disfruta, burlando la acción de la justicia**.**[12]

• Análisis**:** Estudio técnico - científico al lugar de los hechos y a los elementos materia de prueba y evidencia física**.**[13]

• Prueba pericial**:** Medio de prueba legal que consiste en los análisis científicos que realizan los expertos en las diferentes ciencias, disciplinas y artes que aplican a la investigación criminal.[14]

• Embalaje: Es el procedimiento técnico , utilizado para preservar y proteger en forma adecuada los elementos materia de prueba y evidencia física hallados y recolectados en el lugar de los hechos, lugares relacionados y en las diferentes actuaciones de policía judicial , con el fin de ser enviados a los respectivos laboratorios o bodegas de evidencia.[15]

---

[10] FISCALIA GENERAL DE LA NACION. MANUAL DE PROCEDIMIENTOS PARA CADENA DE CUSTODIA. [En Línea] Bogotá "Enero de 2012". [Citado en 23 Marzo de 2016], Disponible en Internet:
< http://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/01/manualcadena2.pdf>

[11] Ibid., p 25

[12] Ibid., p 25

[13] Ibid., p 25

[14] Ibid., p 25

[15] Ibid., p. 25

4.3.1 Norma ISO 27001. Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI).

Esta norma se puede usar para evaluar la conformidad, por las partes interesadas, tanto internas como externas, adoptando el modelo de procesos “Planificar-Hacer-Verificar-Actuar” (PHVA), brindando un modelo robusto para la ejecución de los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad.[16]

4.3.2 Norma ISO 27002. La norma ISO 27002 que anteriormente se denominaba ISO 17799, es un estándar para la seguridad de la información que ha publicado la organización internacional de normalización y la comisión electrotécnica internacional. La versión más reciente de esta norma es la ISO 27002:2013. La norma ISO 27002 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información.

Esta norma se encuentra organizada de la siguiente manera, tiene como base 14 dominios de los que se desglosan 35 objetivos de control y de ellos 114 controles.[17]

[16] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC). Norma técnica NTC-ISO/IEC Colombiana 27001. Bogotá D.C.: 2006 45p.

[17] NORMA ISO 27002: EL DOMINIO POLÍTICA DE SEGURIDAD. [En linea] [Citado en 05 Octubre 2018], Disponible en internet: < https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/>

4.4 MARCO LEGAL

4.4.1 Ley 906 de 2004 (Código Procedimiento Penal)

Artículo 114, Atribuciones # 4.

Artículo 213. Inspección del lugar del hecho.

Artículo 215. Inspecciones en lugares distintos al del hecho.

Artículo 216. Aseguramiento y custodia.

Artículo 254. Aplicación. Con el fin de demostrar la autenticidad de los elementos materiales probatorios y evidencia física, la cadena de custodia se aplicará teniendo en cuenta los siguientes factores: identidad, estado original, condiciones de recolección, preservación, embalaje y envío; lugares y fechas de permanencia y los cambios que cada custodio haya realizado. Igualmente se registrará el nombre y la identificación de todas las personas que hayan estado en contacto con esos elementos.

La cadena de custodia se iniciará en el lugar donde se descubran, recauden o encuentren los elementos materiales probatorios y evidencia física, y finaliza por orden de autoridad competente.

Artículo 255. Responsabilidad. La aplicación de la cadena de custodia es responsabilidad de los servidores públicos que entren en contacto con los elementos materiales probatorios y evidencia física.

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

Artículo 258. Traslado de contenedor. El funcionario de policía judicial o el servidor público que hubiere recogido, embalado y rotulado el elemento material probatorio y evidencia física, lo trasladará al laboratorio correspondiente, donde lo entregará en la oficina de correspondencia o la que haga sus veces, bajo el recibo que figura en el formato de cadena de custodia.

Artículo 259. Traspaso de contenedor. El servidor público de la oficina de correspondencia o la que haga sus veces, sin pérdida de tiempo, bajo el recibo que figura en el formato de cadena de custodia, entregará el contenedor al perito que corresponda según la especialidad.

Artículo 260. Actuación del perito. El perito que reciba el contenedor dejará constancia del estado en que se encuentra y procederá a las investigaciones y análisis del elemento material probatorio y evidencia física, a la menor brevedad posible, de modo que su informe pericial pueda ser oportunamente remitido al fiscal correspondiente.

Artículo 261. Responsabilidad de cada custodio. Cada servidor público de los mencionados en los artículos anteriores, será responsable de la custodia del contenedor y del elemento material durante el tiempo que esté en su poder, de modo que no pueda ser destruido, suplantado, alterado o deteriorado.

Artículo 262. Remanentes. Los remanentes del elemento material analizado, serán guardados en el almacén que en el laboratorio está destinado para ese fin. Al almacenarlo será previamente identificado de tal forma que, en cualquier otro momento, pueda ser recuperado para nuevas investigaciones o análisis o para su destrucción, cuando así lo disponga la autoridad judicial competente.

Cuando se tratare de otra clase de elementos como moneda, documentos manuscritos, mecanografiados o de cualquier otra clase; o partes donde constan números seriales y otras semejantes, elaborado el informe pericial, continuarán bajo custodia.

Artículo 263. Examen previo al recibo. Toda persona que deba recibir un elemento material probatorio y evidencia física, antes de hacerlo, revisará el recipiente que lo contiene y dejará constancia del estado en que se encuentre.

Artículo 264. Identificación. Toda persona que aparezca como embalador y rotulador, o que entrega o recibe el contenedor de elemento material probatorio y evidencia física, deberá identificarse con su nombre completo y apellidos, el número de su cédula de ciudadanía y el cargo que desempeña. Así constará en el formato de cadena de custodia.

Artículo 265. Certificación. La policía judicial y los peritos certificarán la cadena de custodia.

La certificación es la afirmación de que el elemento hallado en el lugar, fecha y hora indicados en el rótulo, es el que fue recogido por la policía judicial y que ha llegado al laboratorio y ha sido examinado por el perito o peritos. Además, que en todo momento ha estado custodiado.

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

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

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

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

4.4.2 Ley 1273 de 2009 Protección de la Información y de los Datos en Colombia. En Colombia existe la ley 1273 con la cual se modificó el código penal y se incluyó en lo relacionado al delito informático, para tener un mejor conocimiento de la ley esta se muestra exacta tal y como se rige:

Por medio de 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” - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

CAPITULO I

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema

informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

• Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

• Por servidor público en ejercicio de sus funciones.

Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

• Revelando o dando a conocer el contenido de la información en perjuicio de otro.

• Obteniendo provecho para sí o para un tercero.

• Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

• Utilizando como instrumento a un tercero de buena fe.

Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPÍTULO II

De los atentados informáticos y otras infracciones

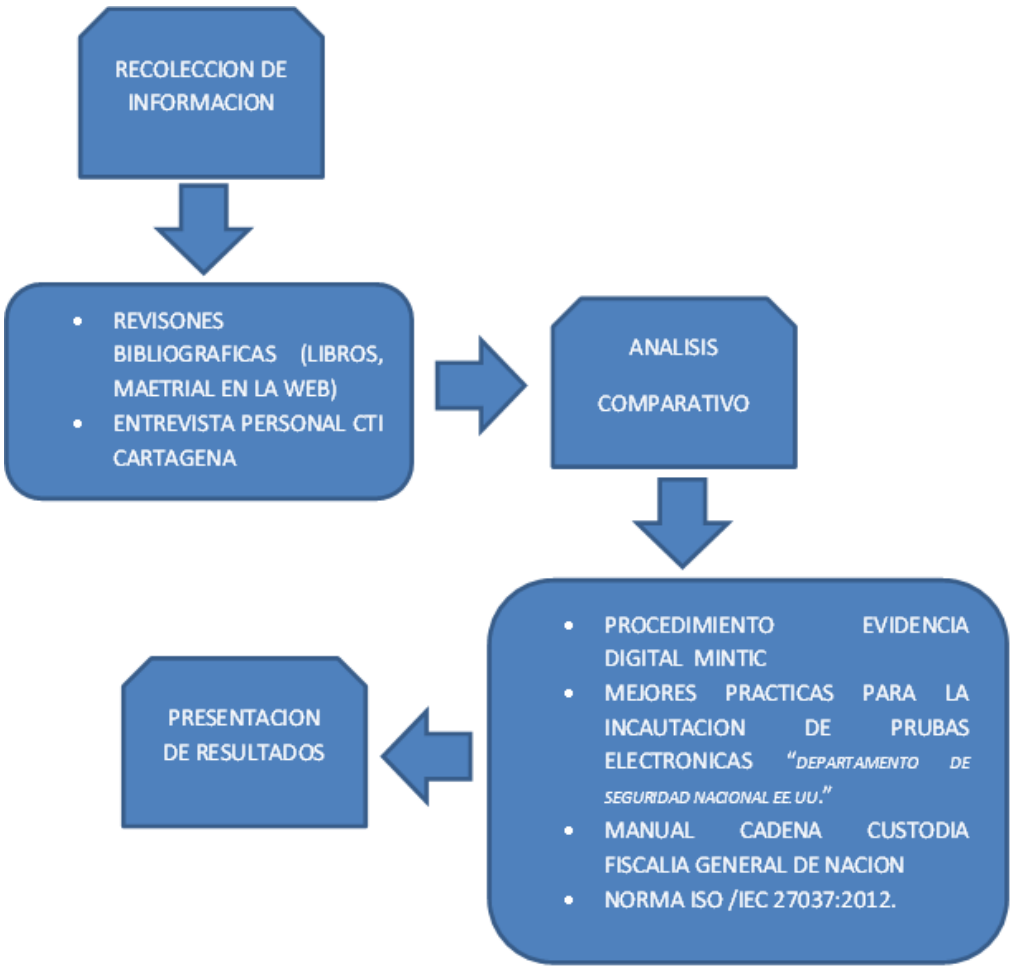
Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

5. MARCO METODOLOGICO

Figura 1. Estructura Metodología



Fuente: El autor.

5.1 DISEÑO DE HIPOTESIS

5.1.1 Hipótesis de Investigación: identificar los factores que pueden afectar la evidencia en el proceso de cadena de custodia en delitos informáticos, permite brindar un soporte eficiente al manejo de pruebas digitales, preservando su valor probatorio.

5.1.2 Hipótesis Nula: identificar los factores que pueden afectar la evidencia en el proceso de cadena de custodia en delitos informáticos, no es posible brindar un soporte eficiente al manejo de pruebas digitales, para que estas puedan preservar su valor probatorio

5.2 UNIVERSO O POBLACION

El universo o población para el estudio a realizar es el procedimiento de cadena de custodia para la evidencia digital en los delitos informáticos en la ciudad de Cartagena.

5.3 MUESTRA

La muestra seleccionada para el estudio es el procedimiento de cadena de custodia realizado a la evidencia digital en la Fiscalía General de la Nación seccional Bolívar, se toma como muestra la sede de la Fiscalía General de la Nación Seccional Bolívar, debido a que es la única entidad en la ciudad de Cartagena que posee una unidad de delitos informáticos.

Para el estudio se analizara de manera general el procediendo que se le debe dar a la evidencia digital según lo que describe el manual para el procediendo de cadena de custodia que dispone la Fiscalía General de la Nación, comparándolo con el

procedimiento para la evidencia digital que establece el ministerio de las tecnologías y comunicaciones - MINTIC.

5.4 TECNICAS PARA LA RECOLECCION DE INFORMACION

Dentro de la estructura de la seccional se encuentra la unidad de delitos informáticos; adscritos al Cuerpo Técnico de Investigación CTI, con el personal de esta unidad se recolectara información de manera directa sobre el procedimiento de cadena de custodia que se realiza cuando se presenta un delito informático y el tratamiento que le dan a la evidencia digital en dicho procedimiento.

Como instrumento de recolección de información se utilizara la entrevista, esta consistirá en realizar unas preguntas a los funcionarios del grupo de delitos informáticos de la seccional Bolívar, en la tabla 1 se evidencia el formato de la entrevista a realizar.

Tabla 1. Formato entrevista

pregunta	respuesta
¿Que realizan ustedes como investigadores cuando llegan a la escena donde se cometió el suceso o incidente?	
¿Cuándo se debe tomar los datos volátiles?	
¿Después de haber recogido la información volátil qué sigue?	

¿Qué procedimiento se realiza al disco duro?	
¿Cómo se preserva la integridad de la imagen forense?	
¿Qué es el hash?	
¿Qué tipo de has utilizan ustedes?	
¿Qué software forense utilizan para el análisis y creación de la imagen forense?	

Fuente: El autor.

5.5 METODOLOGIA DE INVESTIGACION

El tipo de investigación a realizar es de carácter cualitativo – descriptivo, se verificara el proceso de cadena de custodia realizado a la evidencia digital en Fiscalía General de Nación Seccional Bolívar, se recolectara información mediante fuentes primarias como entrevistas al personal del Cuerpo Técnico de Investigación – CTI- seccional Bolívar pertenecientes al grupo de delitos informáticos, observaciones de campo y fuentes secundarias, mediante la consulta de literatura en distintos repositorios de universidades como el de la UNAD, Universidad de Cartagena, entre otras, análisis de trabajos investigativos realizados previamente.

5.6 METODOLOGIA DE DESARROLLO

- Recolectar información acerca del proceso de cadena de custodia de la evidencia digital en delitos informáticos
- Revisión del manual de procedimiento para cadena de custodia elaborado por la Fiscalía General de la Nación.
- Revisión Procedimiento Evidencia Digital elaborado por el Ministerio de Tecnologías de la Información y Comunicaciones de Colombia.
- Identificación de los aspectos significativos para el objeto de la investigación.
- Entrevista al personal del Cuerpo Técnico de Investigaciones - CTI de la Seccional Bolívar ubicados en la ciudad de Cartagena, pertenecientes al área de delitos informáticos.
- Comparar los procedimientos establecidos en los protocolos actuales del proceso de custodia frente a nuevas acciones tipificadas como delitos informáticos.
- Análisis comparativo del procedimiento operativo utilizado por los funcionarios de la unidad de delitos informáticos de la Seccional Bolívar Vs el establecido en el manual de proceso de cadena de custodia de la Fiscalía General de la Nación.
- Realizar cuadro comparativo especificando los procedimientos que actualmente realiza el grupo de delitos informáticos de la Seccional Bolívar para el procedimiento de cadena de custodia y manipulación de la evidencia digital frente al Procedimiento de Evidencia Digital que desarrolló el Ministerio de Tecnologías de la información y Comunicación en Colombia.
- Identificar riesgos presentes en procedimiento realizado para la manipulación de evidencia digital en la seccional.
- Clasificar los riesgos encontrados y plantear una mitigación de los mismos, mediante una serie controles que expone la norma ISO 27002.
- Presentar una serie de recomendaciones a tener en cuenta para la manipulación de evidencia digital.

5.7 METODOLOGIA PARA EL ANALISIS Y CLASIFICACION DEL RIESGO

Para el análisis y clasificación del riesgo se utilizan 2 matrices, la matriz para el análisis y la matriz de clasificación de riesgo, para la matriz de análisis se obtendrán el valor total del riesgo que posteriormente nos permitirá realizar la clasificación del mismo, dependiendo del valor total del riesgo obtenido.

El valor total del riesgo se obtiene como producto de la probabilidad de materialización de la amenaza y el impacto o magnitud si esta llegase a ocurrir. Para las variables de probabilidad e impacto se utiliza una escala de 1 a 4, lo que dará al valor total del riesgo una escala comprendida entre 1 y 16.

Se agrupan tres grupos donde se determinan un nivel de riesgo, en la escala de 1 a 6 se determinan como riesgos de nivel bajo, del rango de 8 a 9 se determinan riesgos de nivel intermedio y del rango de 12 a 16 se determina riesgos de alto nivel.

En la tabla de clasificación de riesgo se encuentra la matriz con tres colores diferentes, verde, amarillo y rojo, estos colores representan los grupos en los que se determinaron el nivel de riesgo, el color verde representa los riesgos de bajo nivel, el amarillo los riesgos de nivel intermedio y los rojos los riesgos de nivel alto. En las celdas de la matriz de clasificación del riesgo se ubican los números correspondiente los ítems que identifican las vulnerabilidades encontradas, que previamente se describen en la tabla de análisis de riesgo.

6. REVISION MANUAL CADENA DE CUSTODIA FISCALIA GENERAL DE LA NACION

6.1 PAUTAS PARA EL TRATAMINETO DE LOS ELEMENTOS MATERIALES PROBATORIOS.

Según el manual de procedimientos para la cadena de custodia de la Fiscalía General de la Nación, se estipulan unas pautas para el tratamiento de elementos materiales probatorios o elementos físicos, desde el aseguramiento del lugar de los hechos, recolección, embalaje y rotulado de los elementos materia de prueba hasta el envío de los mismos ya sea a un almacén transitorio, laboratorio o almacén de evidencias. Se resaltan los siguientes:

- Formato de registro de cadena de custodia
- Rótulo
- Acta de la diligencia respectiva.
- Es obligación de las personas involucradas en el manejo del sistema de cadena de custodia garantizar el diligenciamiento completo del rótulo.
- El rótulo se diligencia con esfero de tinta indeleble, de manera concisa, precisa y exacta, con letra clara, legible y comprensible; su contenido debe ajustarse a la información verdadera y no debe tener enmendaduras ni tachaduras.
- El registro de fecha y hora debe registrase en números arábigos. La fecha se escribe (0000) y la hora en el formato de 00:00 hasta 24:00 horas (hora militar).

En la colocación del rótulo se tiene en cuenta:

- Cuando los EMP (elemento material probatorio) o EF (evidencia física) han sido embalados en bolsas plásticas o de papel, los rótulos diligenciados se adhieren

en el cierre de las mismas, como medida de seguridad a fin de evitar alteraciones de su contenido, de tal manera que al abrir la bolsa se rompa la etiqueta o rótulo. [18]

6.2 MANEJO DE LA EVIDENCIA DIGITAL

Los EMP y EF de tipo digital deben ser embalados en bolsas antiestáticas o materiales que permitan repeler la energía electromagnética. No se deben pasar los EMP y EF por fuentes de este tipo de energía (scanner y detectores de metales, entre otros) para evitar el posible borrado o deterioro de la información en ellos contenida.

Para la recolección e identificación de dispositivos de almacenamiento de información digital y dispositivos móviles, se tendrán en cuenta:

- Marca
- Modelo
- números seriales
- capacidad de almacenamiento
- características morfo-cromáticas entre otras condiciones de identidad.

En caso de extraer discos duros, describir el equipo de cómputo del cual fue obtenido.

Para garantizar la integridad de archivos digitales, en su recolección, se deben emplear programas que permitan calcular valores HASH y almacenarlos en medios que en lo posible no permitan su modificación o daño.

[18] FISCALIA GENERAL DE LA NACION. MANUAL DE PROCEDIMIENTOS PARA CADENA DE CUSTODIA. [En Línea] Bogotá "Enero de 2012". [Citado en 23 Marzo de 2016], Disponible en Internet: < http://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/01/manualcadena2.pdf>

El embalaje de la evidencia digital debe emplear contenedor primario con holgura suficiente para permitir su apertura y posterior sellado por parte de peritos.[19]

6.3 ESQUEMA DE PROCEDIMIENTOS PARA ELEMENTOS MATERIALES PROBATORIOS DIGITALES Y EVIDENCIAS FISICAS

El manual de cadena de custodia de la Fiscalía General de la Nación, establece un esquema donde señala dependiendo el tipo de elemento material probatorio y evidencia física; el estudio requerido, el área de destino, la recolección y embalaje de la evidencia y las precauciones que deben tener para el tratamiento de la misma.

6.3.1 Computadores (Servidores, escritorio y portátiles) y Dispositivos de Almacenamiento digital.

Estudio solicitado:

- Recuperación y extracción de información
- Análisis de código malicioso
- Identificación de cuentas de usuario, sistema operativo y fecha de instalación.
- Programas instalados
- Dirección IP y dominio.
- Cruce de información entre dispositivos

Área Destino:

- Informática forense o el Área que establezca la entidad.

Recolección y Embalaje:

[19] Ibíd. , p. 39

- Si se encuentra encendido y se requiere, obtener datos volátiles mediante software para ese fin; igualmente realizar fijación fotográfica del contenido de la pantalla.
- Se debe desconectar el equipo directamente desde la fuente de alimentación de corriente y si se trata de un portátil se debe quitar la batería embalando todos los elementos tales como adaptador de corriente, cables, batería.
- Si se tiene el conocimiento, extraer el disco duro documentando el equipo de donde se extrae.
- Se debe utilizar dependiendo de la disponibilidad bolsa antiestática, plástica, de papel o caja de cartón, plásticas o acrílicas.
- Siempre que sea posible solicitar contraseñas de descifrado, desbloqueo y acceso a dispositivos.
- Se debe sellar o cubrir las tapas de la torre y las ranuras de inserción de discos, diskettes, CD o DVD.

Precauciones:

- La Evidencia Digital es susceptible a daños a consecuencia de caídas, golpes, vibraciones, exposición a ondas electromagnéticas, altas temperaturas, ralladuras, entre otros.
- No se debe colocar rótulos o adhesivos directamente sobre su superficie.

6.3.2 Celulares

Estudio:

- Recuperación y extracción de información
- Análisis de código Malicioso
- Identificación de cuentas de usuario, sistema operativo, programas instalados.
- Cruce de información entre dispositivos
- Análisis link de comunicación

Área Destino:

- Informática forense o el Área que establezca la entidad.

Recolección y Embalaje:

- Si se encuentra encendido y se requiere, obtener datos volátiles mediante software para ese fin; igualmente realizar fijación fotográfica del contenido de la pantalla.
- Se debe desconectar el equipo directamente desde la fuente de alimentación de corriente y si se trata de un portátil se debe quitar la batería embalando todos los elementos tales como adaptador de corriente, cables, batería.

Precauciones:

- Se debe remitir lo más pronto posible al laboratorio.
- En lo posible embalar el cargador y cable de datos.
- La Evidencia Digital es susceptible a daños a consecuencia de caídas, golpes, vibraciones, exposición a ondas electromagnéticas, altas temperaturas, ralladuras, entre otros.
- No se debe colocar rótulos o adhesivos directamente sobre su superficie.

7. PROCEDIMIENTO EVIDENCIA DIGITAL ELABORADO POR EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE COLOMBIA.

Revisando el documento establece que se deben tener encuentra ciertas medidas al momento de ejecutar el procedimiento de evidencia digital, donde se detallan las siguientes:

- Verificar si existe la necesidad de realizar el procedimiento de evidencia digital al incidente reportado.
- Minimizar la pérdida o alteración de datos.
- Llevar bitácoras de todas las acciones, con fechas y ahora precisas.
- Analice todos los datos recolectados.
- Realice un reporte de los hallazgos[20].

La figura 2 describe de una manera muy sencilla la estructura del Procedimiento de Evidencia digital, detallando las fases del procedimiento de la evidencia digital según el ministerio de las tecnologías y la información, dentro de las cuales se encuentran las fases de aislamiento de la escena, identificación de fuentes de información, examinación y recolección de la información, análisis de datos y por último el reporte.

[20] MINISTERIO DE LAS TECNOLOGIAS Y LA INFORMACION. Seguridad y Privacidad de la Información. Bogotá D.C.: 2016 30 p

Figura 2. Estructura Procedimiento evidencia digital mintic

Fuente: MINISTERIO DE LAS TECNOLOGIAS Y LA INFORMACION. Seguridad y Privacidad de la Información. Bogotá D.C.: 2016 30 p.

7.1 AISLAMIENTO DE LA ESCENA

En esta fase se busca aislar la escena o espacio donde se presenta el suceso, para evitar que esta la evidencia localizada pueda ser contaminada o alterada. En esta fase se deben tener muy claros los siguientes procedimientos:

a) Tomar registro fotográfico del equipo o lugar antes de tocarlo.

b) Establecer un perímetro de seguridad, para que nadie pueda acercarse.

c) Verificar si el equipo se encuentra encendido, si es así no apagarlo y realizar lo siguiente:

- Sellar los puertos USB, *firewire*, Unidades CD/DVD, para impedir alguna alteración posterior al registro de la escena.

- Tomar fotografías de lo que se puede ver en la pantalla (*software* corriendo, documentos abiertos, ventanas de notificación, hora y fecha ilustrados)
- Asegurar el equipo (Si es portátil, tratar de mantenerlo encendido con el cargador hasta hacer entrega o iniciar el análisis respectivo).
- Si es posible capturar información volátil del equipo antes de que se apague, debe hacerse empleando las herramientas forenses necesarias.

d) En el caso de que el equipo se encuentre apagado, no encenderlo, ya que esto puede alterar la escena o borrar información posteriormente podría extraerse.

e) Tener a la mano los elementos o herramientas para la recolección de información como estaciones forenses, dispositivos de *backups*, medios formateados y/o estériles, cámaras digitales, cinta y bolsas para evidencia, papel de burbuja, bolsas antiestáticas, cajas de cartón, rótulos o etiquetas etc….

f) Almacenar la información original en un sitio con acceso restringido, para garantizar la cadena de custodia de la información.

g) Obtener información de dispositivos que tuvieron contacto o interacción con el equipo en cuestión (*switches*, *firewalls*, *Access points* etc…).

7.2 IDENTIFICACIÓN DE FUENTES DE INFORMACIÓN Y ADQUISICIÓN DE DATOS

En esta fase se realiza la identificación de los elementos o materiales que pueden brindar información tales como computadores, servidores, almacenamiento en la red, medios magnéticos, los registros o log del sistema.

Luego de haber identificado las fuentes de información se procede a realizar la adquisición de los datos, la guía describe tres pasos esenciales, que son planificar, adquirir y verificar, en el primero se debe determinar a qué fuentes y en qué orden se les extraerá la información, en segunda instancia es el procedimiento de extracción tanto de información volátil como de información no volátil, luego sigue

la verificación, se debe asegurar que la integridad de la información y que esta no haya sido alterada. Para lograr esto se debe emplear herramientas de cálculo de resumen de mensajes que generan un valor determinado. Dicho valor debe ser igual tanto en la fuente original como en la copia. Esta verificación de integridad se utiliza principalmente para efectos legales, para que la información se certifique como auténtica

Es importante tener en cuenta que si la información va a utilizarse para fines legales, desde el inicio debe tenerse total cuidado con la manipulación, llevando a cabo la cadena de custodia adecuadamente, registrando cada acción, desde que se recolecta, se almacena, se guarda, quien lo hace y la hora exacta, que herramientas se han utilizado para la recolección etc.[21]

7.3 RECOLECCIÓN Y EXAMINACIÓN DE INFORMACIÓN

Una vez se han identificado las posibles fuentes de información, se debe proceder a realizar la recolección y examinación de los datos disponibles.
La secuencia para llevar a cabo la recolección y examinación de medios/información es la siguiente:

- Creación del archivo / bitácora de hallazgos (cadena de custodia). Consiste en la creación y aseguramiento de un documento, ya sea físico o electrónico, que permita llevar un historial de todas las actividades que se llevan a cabo durante el proceso, y de los hallazgos encontrados, de modo que se tenga un resumen que permita hacer la reconstrucción del caso tiempo después de que este haya sido analizado.

[21] Ibíd. , p. 43

- Imagen de datos. consiste en la generación de las imágenes de datos que conciernen al caso en investigación. Se recomienda utilizar herramientas de extracción de imágenes como *Linux dd* o *Encase Forensic Software*.
- Verificación de integridad de la imagen. para cada imagen suministrada se debe calcular su compendio criptográfico (SHA1/MD5), comparándolo luego con el de la fuente original. Si la comparación arroja un resultado negativo se debe rechazar la imagen proveída en el primer paso.
- Creación de una copia de la imagen suministrada. en un análisis de datos nunca se debe trabajar sobre la imagen original suministrada. Debe realizarse una copia master y a partir de esta, se reproducen las imágenes que se requieran.
- Aseguramiento de la imagen original suministrada. se debe garantizar que la imagen suministrada no sufra ningún tipo de alteración, con el fin de conservación de la cadena de custodia y del mantenimiento de la validez jurídica de la evidencia.

8. ENTREVISTA PERSONAL UNIDAD DE DELITOS INFROMATICOS CTI SECCIONAL BOLIVAR

Los días 23 y 24 del mes de octubre de 2017 se concretó una reunión con 2 funcionarios de cuerpo técnico de investigación del CTI, adscritos a la planta de personal de la Seccional Bolívar, específicamente con Luis Felipe González Rubio y Roberto Tinoco, con cargos de Técnico Investigador II y Técnico Investigador I respectivamente, dichos funcionarios se encuentran asignados a él aérea de delitos informáticos de la Seccional, siendo Luis Felipe González Rubio coordinador de esta dependencia.

Comencé la entrevista preguntando sobre la fase de aseguramiento de la escena donde se comete el delito.

Tabla 2. Entrevista realizada.

Pregunta	Respuesta
¿Que realizan ustedes como investigadores cuando llegan a la escena donde se cometió el suceso o incidente?	Hay ciertas pautas o tics en cuanto a las técnicas de recolección, como quitarse cualquier medio metálico que pueda causar alguna interrupción con la corriente, colocarse unos guantes de látex o caucho y en lo posible colocarse manilla antiestática, documentar la manera como se encuentra el equipo, si se encuentra un computador de escritorio o portátil encendido no trabajar sobre el equipo, si se requiere se procede a tomar la información de datos volátil.

Tabla 2. (Continuación)

Pregunta	Respuesta
¿Cuándo se debe tomar los datos volátiles?	se debe tener en cuenta la línea investigativa y en base a eso se determina si se necesitan o no los datos o información volátil, cuando se quiere coger una flagrancia, si se quiere verificar si se está cometiendo un delito en ese mismo momento, se revisa que se estaba trabajando en el momento en el equipo, mediante los procesos que se estaban ejecutando, si estaba conectado a internet a cierta página, si estaba revisando algún documento de Word o cualquier cosa pero todo dependiendo de lo que se esté manejando en la investigación. El perito indica que lo primero es realizar la extracción de datos volátiles siempre y cuando vaya acorde a la línea de investigación y resalta que es de suma importancia en este procedimiento es que todo vaya bien documentado por que indica el que para la recolección de datos volátiles de una u otra forma se debe manipular el equipo, ya que para recolectar es necesario conectar memoria USB,

Tabla. 2 (Continuación)

Pregunta	Respuesta
	Utilizar algún tipo de software para dicho proceso, el hace referencia al software Encase indicando que este tiene una versión portable, que con esta la conectan al equipo mediante una USB y este automáticamente realiza la recolección de los datos volátiles. Luego que se recolecta esta información temporalmente ya que en muchas veces no se cuenta para quemar o guardar información un cd, se guarda en un medio externo y cuando llegan a la oficina se procede a guardar en un medio magnético para abrir cadena de custodia.
¿Después de haber recogido la información volátil qué sigue?	Dependiendo si es un computador de escritorio o si es un portátil, si es un computador de escritorio enseguida se desconecta de la corriente y se hace la recolección del disco duro, documentando todo el proceso, indicando marca, serial, modelo, etc., fotografiar donde se encuentra el disco duro, esto sirve para presentar en audiencia más adelante, luego de que se recolecta se hace el embalaje, como es un medio magnético, se utiliza bolsa antiestática para protegerlo de las radiaciones electromagnéticas.

Tabla. 2 (Continuación)

Pregunta	Respuesta
	Si es un computador portátil, como la idea es dejarlo sin corriente aquí lo que toca es quitar la batería, se desconecta la batería y se realiza el apagado abrupto del equipo, luego de esto se realiza el mismo procedimiento, se destapa el equipo para realizar la extracción del disco duro, documentando todo y tomando registro fotográfico para proceder con el embalaje del disco.
¿Qué procedimiento se realiza al disco duro?	Se envía al laboratorio forense, el cual dispone de un procedimiento o protocolo para preservar la integridad de la información o los datos contenidos en el disco duro. Se realiza una imagen forense, esto consiste en una copia bit a bit del disco, para realizar esta copia no se realiza directamente en el equipo al que se le va realizar la imagen, el dispositivo de almacenamiento se conecta al bloqueador de escritura y eso se conecta al equipo, con el software forense se genera la imagen
¿Cómo se preserva la integridad de la imagen forense?	El software forense genera un hash, uno de adquisición y uno de verificación, ambos deben coincidir, al coincidir esto indica que la imagen se hizo correctamente y que no sé

Tabla. 2 (Continuación)

Pregunta	Respuesta
	ha alterado la información por lo tanto la evidencia se preservo
¿Qué es el hash?	Es la ejecución de un algoritmo que por decir así un código alfanumérico y ese código va a identificar un archivo. Hay diferentes tipos de hash, siendo el más común el MD5, aunque ya está el SHA1, SHA256, CRC32.
¿Qué tipo de has utilizan ustedes?	SHA1 Y MD5
¿Qué software forense utilizan para el análisis y creación de la imagen forense?	Encase

Fuente: El autor

9. COMPARACION DE PORCESOS SEGÚN EL PROCEDIMIENTO DE EVIDENCIA DIGITAL ESTABLECIDO EN LA GUIA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION, ELABORADO POR EL MINISTERIO DE LAS TECNOLOGIAS Y COMUNICACIÓN - MINTIC

En esta instancia se pretende mediante tablas de relación hacer una comparación de los procesos ejecutados por el personal que gestiona en el área de delitos informáticos de la seccional Bolívar vs los procedimientos de la guía de seguridad y privacidad de la información, elaborado por el ministerio de las tecnologías y comunicación - MINTIC, dejando evidenciado que tan ajustados se encuentran a dicha guía.

El análisis comprenderá las fases de aislamiento y adquisición, en las tablas se detallan en una fila los procesos que expone el estándar o guía y en la columna del borde izquierdo de la tabla los realizados por el área de delitos informáticos de la seccional Bolívar, se marcara con un color amarillo si el procedimiento realizado por el área de delitos informáticos de la Seccional encaja en algunos de los descritos en la guía para la fase correspondiente.

Tabla 3. Fase aislamiento equipo apagado

COMPARACION FASE AISLAMIENTO EQUPO APAGADO

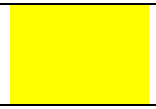
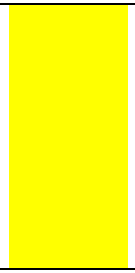
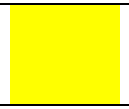
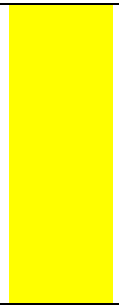
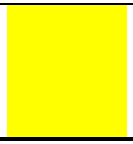
Guía MINTIC / PRO CTI	Registro fotográfico previo del lugar	Establecer Perímetro	No encender Equipo	Contar con Estación Forense	Medios Estériles	Bolsas Antiestáticas	Bolsas Para evidencia	Rótulos o Etiquetas	Cajas de cartón
Despojarse de prendas metálicas									

Colocarse manillas antiestáticas	
Identificar si es un desktop o laptop	
Estación forense portátil	
Utilizar bolsas antiestáticas	
Rotular lo que sea necesario	
Utilizar dispositivos formateados para almacenamien o de información si es requerido	
Documentar como se encuentra el equipo	
Dejar el equip apagado preferiblement desconectar cable de poder o extraer bater si es equipo portátil.	

Fuente: El autor.

Tabla 4. Fase aislamiento equipo encendido

COMPARACION FASE AISLAMIENTO ESTANDO EQUIPO ENCENDIDO													
GUIA MINTIC / PRO CTI	Registro fotográfico previo del lugar	Establecer Perímetro	Sellar Puertos USB	Sellar unidades CD/DVD	Registro Fotográfico de lo observado en pantalla	Mantener equipo encendido	Capturar información volátil	Contar con Estación Forense	Medios Estériles	Bolsas Antiestáticas	Bolsas Para evidencia	Rótulos o Etiquetas	Cajas de cartón
Despojarse de prendas metálicas													
Extraer información volátil(dependiendo de la línea investigativa)													
Colocarse manillas antiestáticas													
Identificar si es un desktop o laptop													
Estación forense portátil													

Utilizar bolsas antiestáticas	
Mantener equipo encendido (si se requiere extraer información volátil)	
Rotular lo que sea necesario	
Utilizar dispositivos formateados para almacenamiento de información si es requerido	
Documentar como se encuentra el equipo	

Fuente: El autor

Tabla 5. Fase adquisición

COMPARACION FASE ADQUISICION								
Guía mintic / Pro cti	Creación de bitácora	Generación de imagen de datos	Calcular compendio criptográfico (md5/sha1)	Copia imagen master	Descartar que la imagen tenga virus	Estación forense	Nunca trabajar sobre imagen original	Obtener información con estampa de tiempo precisa
Recolectar disco Duro								
Fotografiar donde se encuentra el disco duro								
Documentar proceso de extracción del disco(marca, modelo , Serial)								
Realizar copia Bit a Bit del disco								
Utilizar bloqueador de escritura								
No se realiza la copia directamente en el equipo implicado								
Generar Hash a la imagen, se utilizan MD5 y SHA1								
Estación forense software encase								

Fuente: El autor

10. RESULTADOS DE ESTUDIO REALIZADO

Tabla 6. Hallazgos de Riesgos

Hallazgo	Descripción riesgo
No uso de bolsas *Faraday*	El no uso de bolsas *Faraday* para la recolección o extracción de dispositivos móviles en la escena del incidente, ya que el trato que se le aplica a estos elementos es el procedimiento general para los elementos físicos, recolectar y embalar para enviar al laboratorio, en ese transcurso al dispositivo no se le deja bloqueado o se interrumpe la señal, dejando abierta una oportunidad para que pueda ser accedido remotamente y sea alterado su contenido.
Calculo Valores HASH	En el manual de Cadena de Custodia de la Fiscalía General de Nación se estipula que se deben usar programas que permitan el cálculo de funcionas *HASH*, con el fin de garantizar la integridad de archivos digitales pero no se estipula que funciones se deben utilizar.
Función HASH MD5	Se tiene que la función MD5 a pesar de que hoy en día es utilizada frecuentemente, esta se encuentra muy vulnerable a diversos ataques, por ejemplo el de colisión y colisión de prefijo elegido,

Tabla 6. (Continuación)

Hallazgo	Descripción del riesgo
	Dejando validar distintos elementos con un mismo hash lo que le resta confiablidad a la imagen que se presente con dicho hash, lo que permitiría que la evidencia perdiera valor probatorio.
Función HASH SHA1	Esta función presenta las mismas falencias de la función MD5, en menor escala pero de igual manera las presenta, se toma esto como un riesgo a la integridad de la evidencia y que esta pierda su valor probatorio.

Fuente: El Autor

10.1 ANALISIS Y CLASIFICACIÓN DE LOS RIESGOS ENCONTRADOS

Habiendo identificado los riegos detallados en la tabla 6, se procederá a realizar una evaluación de dichos riesgos mediante el estándar ISO 27001 e ISO 27002, con el fin de cuantificar el impacto que estos podrían tener y el tratamiento a seguir.

Se determinara mediante la probabilidad de ocurrencia y el impacto, se le dará valor numérico en escala de 1 a 4, siendo 4 el valor más alto.

Para la impacto estableceremos para todos los hallazgos un valor de 4, ya que estos siempre que se presenten tendrían una magnitud muy alta de que la evidencia pierda su valor probatorio.

El cálculo total de riesgo se determinara mediante la multiplicación de los valores de probabilidad e impacto, teniendo como escala valores entre 1 y 16 como máximo, siendo este un valor crítico.

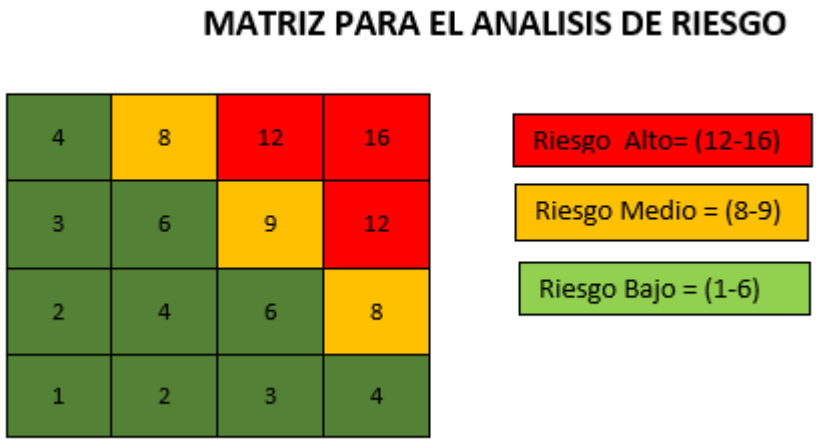
10.1.1 Análisis del Riesgo

Tabla7. Análisis de Riesgo

Ítem	Vulnerabilidades	Amenaza	Riesgo	Probabilidad				Impacto				Valoración Total del Riesgo
				1	2	3	4	1	2	3	4	
1	No uso de bolsas Faraday	Ataques externos, Acceso no autorizado conexión remota	Alteración, eliminación de información.		X						X	8
2	Calculo Valores HASH.	Uso función inadecuada u obsoleta.	Perdida integridad imagen realizada.			X					X	12
3	Función HASH MD5	Ataques de colisión y colisión de prefijo elegido	Perdida integridad imagen realizada.				X				X	16
4	Función HASH SHA1	Ataques de colisión y colisión de prefijo elegido	Perdida integridad imagen realizada.			X					X	12

Fuente: El Autor

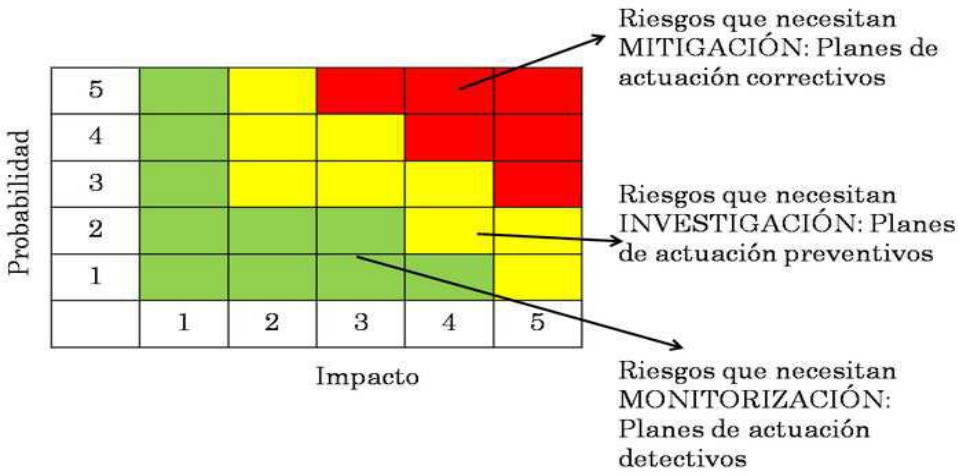
Figura 3. Matriz para el análisis de riesgo.



Fuente: El Autor

En la figura 3 se describe la matriz para el análisis de riesgo, se cuantifica el riesgo como producto de la magnitud del daño en relación con la probabilidad de amenaza.

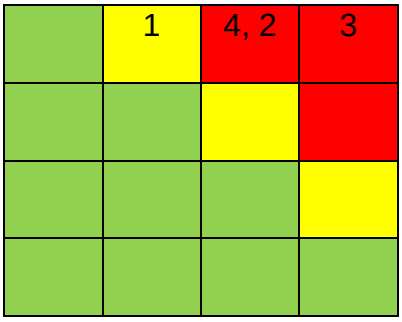
Figura 4. Descripción matriz análisis de riesgo.



Fuente: ERB, M. (2008). Gestión de Riesgo en la Seguridad Informática.

10.1.2 Clasificación del Riesgo

Tabla 8. Matriz Clasificación Riesgo



Fuente: El Autor

En la tabla 8 se especifican los riesgos según su valoración para determinar las actividades a seguir. Los números en la matriz hacen énfasis a los ítems descritos en la tabla 7.

Tabla 9. Clasificación de los riesgos

Ítem	Riesgo	Clasificación del Riesgo
1	Alteración, eliminación de información.	Riesgos que necesitan Investigación: Planes de actuación Preventivos. Mejorar condición.
2, 3, 4	Perdida integridad imagen realizada.	Riesgos que necesitan Mitigación: Planes de actuación correctivos, Gestión Urgente.

Fuente: El Autor.

Tabla 10. Tabla estructuración tratamiento de los riesgos.

Ítem	Riesgo	Clasificación del riesgo	Control de Mitigación de Riesgo	Detalle del control – técnica y mecanismo	Justificación- referente, quien lo implementa, cuando, y costo
1	Alteración, eliminación de información.	**Riesgos que necesitan Investigación: Planes de actuación Preventivos. Mejorar condición.**	**Dominio:** 5. Políticas de Seguridad **Objetivo de Control: 5.1.** Directrices de la dirección en seguridad de la información. **Control: 5.1.2** Revisión de las Políticas para la seguridad de la información	Revisar periódicamente las herramientas con las que cuentan el laboratorio informático forense y el plan de adquisición de las mismas.	Las directrices se deben fijar desde la subdirección seccional del Cuerpo Técnico de Investigación y mediante el funcionario de control interno realizar revisión semestral del cumplimiento de las directrices. El coordinador del área del laboratorio debe realizar reporte de las necesidades tecnológicas al asesor del Cuerpo Técnico de Investigación – CTI de la seccional.
2 **3** **4**	Perdida integridad imagen realizada	**Riesgos que necesitan mitigación: Planes de actuación correctivos, Gestión**	**Dominio:** 10. Cifrado **Objetivo de Control:** 10.1 Controles Criptográficos. **Control:** 10.1.1 Políticas de uso de los controles criptográficos.	Establecer políticas de uso de funciones hash seguras y mediante auditoria de control interno verificar que están se cumplan.	Las políticas se deben fijar desde la subdirección seccional del Cuerpo Técnico de Investigación y mediante el funcionario de control interno realizar revisión semestral del cumplimiento de las políticas.

Fuente: El Autor.

11. RECOMENDACIONES

11.1 RECOMENDACIONES PARA EL MANEJO DE EVIDENCIA DIGITAL

11.1.1 Fase previa

- Disponer de los elementos o utensilios (contenedores, herramientas antiestáticas, *pendrive*, maletín forense, cintas, *stiker* para identificación)

11.1.2 Fase identificación

- Registrar fecha y hora cuando se llega al lugar
- Tomar registro fotográfico del lugar y dispositivos encontrados.
- Aislar la escena o lugar del incidente, se debe establecer el cierre por lo general con cintas del perímetro donde se encuentran los equipos o dispositivos encontrados.
- Si se encuentran equipos encendidos y se requiere o determinan que se debe extraer información volátil, se debe tener en cuenta:

1. No apagar el equipo
2. Tomar registro fotográfico del equipo
3. Desconectar cable red o apagar dispositivo wifi
4. Sellar todos los puertos del equipo que no estén en uso.

- De lo contrario cuando no se va a extraer información volátil se debe:

1. Tomar registro fotográfico
2. Desconectar cable de poder si es equipo de escritorio o extraer batería si es dispositivo móvil, no se debe realizar el proceso de apagado desde el sistema o mediante el botón manual.

11.1.3 Fase Colección

- Para el proceso de extraer información volátil, documentar cada paso, desde quien es el especialista encargado, *software* utilizado, fecha y hora de inicio, fecha hora fin, procedimiento utilizado, ya que para esto se manipula el equipo lo que podría alterar procesos, así que todo debe quedar documentado.

- Para el embalaje de los contenedores digitales, como CD, discos duros, pendrive utilizar bolsa antiestática.
- Para los dispositivos móviles como celulares y tabletas, utilizar bolsas *Faraday*.
- Etiquetar todo material a embalar.

11.1.4 Fase de extracción y verificación

- Uso de *software* forense.
- Realizar copia de bits a bits.
- nunca trabajar sobre la imagen original.
- Calcular hash para las imágenes.
- Si utilizan funcionen hash md5 o sha1, calcular ambas para la misma imagen y concatenar el valor arrojado.

12. RESULTADOS

Para el día 20 de Noviembre del año 2018 se consigue ser atendido por el personal del cuerpo técnico de investigación – CTI adscritos a la seccional Bolívar, en una pequeña charla de unos 40 minutos aproximadamente se les enseña el folleto guía para el manejo de la evidencia digital que se encuentra en el anexo A, se socializan los puntos expuestos en la guía, se intercambian conceptos y se hace entrega del folleto, en la figura 5 se evidencia entrega del mismo, al investigador Roberto Tinoco asignado a la unidad de delitos informáticos de la seccional.

Figura 5. Entrega Folleto

Fuente: El autor.

13. CONCLUSIONES

- Se realizó estudio de vulnerabilidades al proceso de cadena de custodia de las evidencias digitales en los delitos informáticos en la ciudad de Cartagena, tomando como muestra el procedimiento realizado por la unidad de delitos informáticos del Cuerpo Técnico de Investigación – CTI Seccional Bolívar, identificando 4 vulnerabilidades al proceso que esta unidad realiza, se establece un tratamiento para los riesgos identificados permitiendo generar unas recomendaciones para la mitigación de los mismos.

- Se recolectó información acerca del proceso de cadena de custodia que se le da a la evidencia digital mediante entrevista que se realizó con los investigadores del área de delitos informáticos del cuerpo técnico de investigación – CTI, adscrito a la Fiscalía General de la Nación Seccional Bolívar, se pudo tener conocimiento del procedimiento que se le da a la evidencia digital.

- Habiendo conocido por parte de los investigadores y verificando el manual que establece la entidad para el proceso de cadena de custodia, se comparó dicho procedimiento con el expedido por el ministerio de tecnologías y comunicación – MINTIC, permitiendo identificar 4 vulnerabilidades que tienen que ver con el no uso de bolsas Faraday para la recolección de dispositivos móviles y las funciones HASH que se utilizan para la preservación de la imagen que se realizan de los discos colectados.

- Se presentaron los resultados que arrojó el estudio realizado, se tomaron las 4 vulnerabilidades encontradas que representaban 2 riesgos, se adoptaron los controles según la norma ISO 27002 que se asocian al área de los riesgos identificados para establecer el tratamiento de los mismos y así conseguir

mediante las actividades sugeridas la mitigación de dichos riesgos. Para tal fin se describen una serie de recomendaciones para tener en cuenta en el proceso para el manejo de la evidencia digital y se realiza una guía como especie de folleto para que de una manera más tangible se pueda impactar la mitigación de los riesgos identificados Recolectar información acerca del proceso de cadena de custodia de la evidencia digital en delitos informáticos, mediante métodos de investigación, para recolección y custodia de la evidencia, como posible elemento probatorio

BIBLIOGRAFIA

ACURIO DEL PINO, Santiago. MANUAL DE MANEJO DE EVIDENCIAS DIGITALES Y ENTORNOS INFORMÁTICOS. [En Linea] “07 de Julio de 2009”. [Citado en 20 de Octubre de 2016], Disponible en internet:<http://www.oas.org/juridico/english/cyb_pan_manual.pdf>

ALCALDÍA DE BOGOTÁ. Ley 906 de 2014 [En línea], Bogotá “1 de Septiembre de 2004”. [Citado en 25 Marzo de 2016], Disponible en Internet: < http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=14787>

ARBOLEDA MURRILLO, Henry, et al. CADENA DE CUSTODIA, SU TRASCENDENCIA Y APLICACION EN SISTEMA PENAL ACUSATORIO DURANTE 2005-2006 [En Línea], Manizales “2007”. [Citado en 23 Marzo de 2016], Disponible en Internet:

<http://ridum.umanizales.edu.co:8080/xmlui/bitstream/handle/6789/523/140_Murillo_Arboleda_Henry_2007.pdf?sequence=1>

CORTES, Jose Bernardo. Manejo de evidencia digital en dispositivos de almacenamiento pendrive usb aplicando la norma iso/iec 27037:2012. Trabajo de grado Especialista Seguridad Informática. Cartagena D.T.C. Universidad Nacional Abierta y a Distancia. Facultad de Ingeniería. Escuela de Ciencias Básicas y Tecnologías. 2014. 59 p.

Deconceptos.Com. CONCEPTO DE PERITO [En Línea]”s.f.”[Citado 25 de Marzo de 2016], Disponible en internet: < http://deconceptos.com/ciencias-naturales/perito>

FISCALIA GENERAL DE LA NACION. MANUAL DE PROCEDIMIENTOS PARA CADENA DE CUSTODIA. [En Línea] Bogotá "Enero de 2012". [Citado en 23 Marzo de 2016], Disponible en Internet: < http://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/01/manualcadena2.pdf>

GAVIRIA, Pablo. PROPUESTA DE UN MODELO DE PROCEDIMIENTO PARA EL TRATAMIENTO DE LA EVIDENCIA DIGITAL, ACORDE A LA NORMATIVIDAD COLOMBIANA SOBRE DELITOS INFORMÁTICOS. [En Línea] Pasto “Enero 10 de 2015” [Citado en 26 Abril de 2016], Disponible en internet: < http://hdl.handle.net/10596/4008>

HENAO NOREÑA, Juan. LA CADENA DE CUSTODIA EN EL SISTEMA PENAL ACUSATORIO [En línea], Medellín “2012”. [Citado en 23 Marzo de 2016], Disponible en internet:http://repository.udem.edu.co/bitstream/handle/11407/277/La%20cadena%20de%20custodia%20en%20el%20Sistema%20Penal%20Acusatorio.pdf?sequence=1>

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC). Norma técnica NTC-ISO/IEC Colombiana 27001. Bogotá D.C.: 2006 45p.

MINISTERIO DE LAS TECNOLOGIAS Y LA INFORMACION. Seguridad y Privacidad de la Información. Bogotá D.C.: 2016 30 p.

NORMA ISO 27002: EL DOMINIO POLÍTICA DE SEGURIDAD. [En linea] [Citado en 05 Octubre 2018], Disponible en internet: < https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/>

SANTOS TELLO, Jorge. PROCEDIMIENTOS EN LA INVESTIGACIÓN, RECOLECCIÓN Y MANEJO DE LA EVIDENCIA DIGITAL EN LA ESCENA DEL CRIMEN. [En linea] Hueheutango “Septiembre de 2013”. [Citado en 28 Marzo 2016], Disponible en internet: < http://biblio3.url.edu.gt/Tesario/2013/07/03/Santos-Jorge.pdf>

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD. [En Linea] (s.f.). [Citado en 23 de Marzo de 2016], Disponible en internet:< http://campus03.unad.edu.co/ecbti04/mod/lesson/view.php?id=10442>

TECNOLÓGICO DE ANTIOQUIA. (2012). ISSN 2027-8101. Núm 3. *Revista ACTIVA,* 67-81.

ANEXO A

https://drive.google.com/open?id=1sBqBoidV52f5kMlNzLYtn_igkF6HAcDi