EL TRATAMIENTO DE LA EVIDENCIA DIGITAL, UNA GUÍA PARA SU ADQUISICIÓN Y/O RECOPILACIÓN

THE TREATMENT OF DIGITAL EVIDENCE, A GUIDE TO ITS ACQUISITION AND/OR COLLECTION

Fecha de recepción: 28 de febrero de 2018.
Fecha de aceptación: 2 de junio 2018.

Código JEL: M4, M41
Código DOI: 10.25097/rep.n28.2018.03

Paúl A. Ochoa Arévalo[1]
paul.ochoaa@ucuenca.edu.ec

Resumen

El tratamiento de la evidencia digital constituye un pilar fundamental en la investigación forense; razón por la cual, se analizan los principales marcos de mejores prácticas existentes y su aplicación a un proceso de investigación digital en nuestro país, de manera que fundamente una propuesta para el debido tratamiento de evidencia para la adquisición y/o recopilación, la cual abarca las actividades de: identificación, recolección y/o recopilación, resguardo y traslado.

Palabras Clave: evidencia digital, computación forense, seguridad de la información, adquisición de evidencia digital, recopilación de evidencia digital.

Abstract

The treatment of digital evidence becomes the foundation of forensic research. For this reason, we analyze the best existing practices and its application to a digital investigation process in our country. This will be the basis that supports our proposal for the correct evidence treatment of acquisition, which implies: identification, collection, acquisition, and preservation.

Keywords: digital evidence, forensic computing, information security, acquisition of digital evidence, collection of digital evidence

1 Facultad de Ciencias Económicas y Administrativas, Universidad de Cuenca, Av. 12 de abril y Av. Loja, Cuenca, Ecuador

1. Introducción

No cabe duda del papel fundamental que juegan los Sistemas de Información y las Tecnologías de la Información en la sociedad actual; este aspecto ha provocado que se materialicen oportunidades de negocio nunca pensadas sin el desarrollo de la tecnología. Sin embargo, este entorno que se encuentra lleno de oportunidades también cuenta con un sin número de riesgos como el crimen cibernético, el cual presenta un reto debido a la velocidad, anatomía y volatilidad de la evidencia digital. Es por esta razón que se hace necesario enfrentarlo este riesgo de una manera estructurada e integral.

Según estudios de la empresa especialista en ciberseguridad Trustwave (Trustwave, 2018), en su reporte "Global Security Report" liberado en abril de 2018, se dio a conocer los diferentes tipos de compromisos, sectores afectados, así como los métodos de ataque y detección de incidentes. El resultado de este estudio se basa en el análisis de los principales compromisos de seguridad durante el 2016, cuyas fuentes comprenden: investigación de compromisos, información de los centros de operaciones de seguridad, escaneos de red, análisis de transacciones web y ejecución de pruebas de penetración a bases de datos, redes y aplicaciones.

Así, las brechas de seguridad en América Latina comprometieron la información en un 4% en 2017, comparado con el 10% en 2016 de los casos analizados; de los cuales el 50% se dan en la red interna corporativa, el 20% corresponde a puntos de venta POS y el 30% a comercio electrónico.

Identificando entre los principales métodos de ataque:

- Pishing / Ingeniería Social
- Acceso remoto
- Empleados malintencionados
- Inyección de código
- Fallas en la configuración
- Carga de archivos
- Malware

Siendo detectados solamente el 43% por la misma empresa; lo que indica que las empresas deben estar preparadas para gestionar los incidentes de seguridad. De este modo, se puede concluir que este proceso es de vital importancia, tal cual lo indica la norma ISO 27002:2013 respecto a la necesidad de contar con procedimientos para el manejo de evidencia digital.

Además, según el Foro Económico Mundial, los ciberataques para el 2017 forman parte de los tres principales riesgos para la economía global. En este contexto, los ciberataques a empresas se han duplicado en los últimos 5 años afectando principalmente a infraestructuras críticas y sectores estratégicos de la industria.

También hay que resaltar que en el Ecuador, el Código Orgánico Integral Penal, sanciona los delitos contra la seguridad de los activos de los sistemas de información y comunicación, siendo estos: revelación ilegal de bases de datos, interceptación ilegal de datos, transferencia electrónica de activo patrimonial, ataque a la integridad de sistemas informáticos, delitos contra la información pública reservada legalmente, acceso no consentido a un sistema informático, telemático o de telecomunicaciones. De igual manera reconoce al contenido digital como "todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático", asimismo, dentro del proceso investigativo se debe cumplir con reglas respecto a la necesidad del uso de técnicas forenses para el análisis, valoración, recuperación y representación del contenido digital.

Finalmente, si bien las fases de computación forense de manera general, se dividen en: adquisición y/o recopilación, examen, análisis y reporte; el enfoque de la presente guía se centra en los principios bases para la fase de adquisición y/o recopilación. De cierto modo, esta fase es la más importante, debido a que solo tenemos una oportunidad para ejecutarla; por lo tanto, se requiere un enfoque estructurado para su tratamiento, el cual incluye actividades base bien definidas y ejecutadas por personal debidamente capacitado con herramientas tanto de hardware y software probados y licenciados de ser el caso.

2. Materiales y métodos

Se realiza un análisis comparativo entre los principales estándares existentes en la actualidad para el manejo de evidencia digital, los cuales se detallan en sección posterior y se efectúa un estudio de caso (Banco Del Austro, S.A., v. Wells Fargo Bank, 2016); el mismo que trata sobre uno de los casos más relevantes seguidos por un Banco ecuatoriano en los Estados Unidos, debido a transferencias enviadas desde el 12 al 21 de enero de 2015 por un monto aproximado de $12'.000.000, usando la red internacional de pago Swift, dichas transferencias tuvieron principales beneficiarios en Estados Unidos y Hong Kong; el estudio de caso es particularmente útil dentro del área de Tecnología de la Información, debido a que nos permite el estudio de un fenómeno en su estado natural. El estudio de un único caso es apropiado cuando este representa un caso de prueba para una teoría bien definida. De esta manera, un caso de estudio es usado para el análisis y propuesta de tratamiento de evidencia digital, debido al manejo adecuado de la evidencia que permitió la presentación de esta en la corte, seguros y reaseguros e investigaciones por parte de organismos tales como: Swift y FBI (Federal Bureau of Investigation).

2.1 Definición de la computación forense

El Doctor H.B. Wolfe la define como "una serie metódica de técnicas y procedimientos para recopilar evidencia, desde equipos informáticos y diversos dispositivos de almacenamiento y medios digitales, que pueden presentarse en un tribunal de justicia en un formato coherente y significativo. (Anthony Reyes, 2007)

El NIST (National Institute of Standards and Technology) (Timothy Grance, 2006) la define como la aplicación de la ciencia a la identificación, recopilación, examen y análisis de datos, al tiempo que se preserva la integridad de la información y se mantiene una estricta cadena de custodia de los datos.

Según el Standard and Principles Scientific Working Group on Digital Evidence (SWEDGE) (SWEDGE, 2018) la evidencia digital es cualquier información con valor probativo que es almacenada o transmitida en forma digital.

La evidencia digital la podemos clasificar en dos tipos:

- Volátil: hace referencia a información temporal, como la que reside en la memoria principal (RAM).
- No volátil: hace referencia a memoria permanente tales como discos duros, usb's, cd's, etc.; esta información se mantiene cuando se apaga el equipo.

2.2 Reglas de Evidencia

Existen cinco reglas que gobiernan la evidencia digital, necesarias de tomar en consideración cuando se recolecta evidencia digital; dichos principios, permiten conocer qué se puede y no hacer cuando se trata con evidencia digital.

La evidencia digital tiene la característica de ser volátil y fácilmente manipulable, siendo vital considerar los siguientes principios (Sheetz, 2013) que permiten que sea válida en los tribunales de justicia.

1. Admisible. - La evidencia debe poder ser utilizada en la corte.

2. Auténtica. - La evidencia debe ser real y relacionarse con el incidente de manera relevante.

3. Completa. - La evidencia debe ser suficiente, demostrar una perspectiva integral del incidente y poder probar las acciones o inocencia del atacante.

4. Confiable. - La evidencia que se recolecta y posteriormente se analiza, no debe causar duda de su autenticidad y veracidad; en otras palabras, contar toda la historia.

5. Creíble. - La evidencia debe ser claramente entendible y convincente para un jurado.

Como guía para el cumplimiento de los principios se han desarrollado estándares para la recolección y preservación de la evidencia digital; estos estándares han sido desarrollados por algunas organizaciones, los mismos que de manera general confluyen en:

- La evidencia original debe ser preservada en el estado más cercano al que fue encontrado.
- Las personas que ejecuten las actividades de adquisición o recopilación de la evidencia deben ser debidamente capacitadas para el efecto.
- Crear una copia exacta (imagen) de la evidencia original, la cual debe ser usada para efectuar las operaciones de análisis.
- Las copias que se realicen deben ser realizadas en medios limpios; es decir, que no exista información previa.
- Toda la evidencia debe ser etiquetada, documentada de manera apropiada y la cadena de custodia preservada. La cadena de custodia es de extrema importancia, debido a que indica: quién tiene acceso al dispositivo en cualquier momento en el tiempo, usualmente contiene los registros de bitácora de la recolección, manejo, trasporte, almacenamiento y cambios de custodio.

2.3 Modelos para el tratamiento de evidencia digital

A continuación, se analizan 3 modelos ampliamente usados y difundidos en todo el mundo:

2.3.1 Guía para equipos de primera respuesta (Justice, 2008)

El departamento de justicia de los Estados Unidos publicó la guía “Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition”, la cual tiene como objeto asistir a los equipos de primera respuesta los cuales son los responsables de la identificación, recopilación / adquisición y protección de la evidencia digital. Esta guía cubre las fases de:

1. Documentación de la escena: abarca las actividades de fijación fotográfica y etiquetado de la evidencia que permita recrear la escena posteriormente. La documentación debe incluir el tipo, localización, posición de los equipos, componentes, periféricos, etc.

2. Recopilación de evidencia: de manera que se mantenga la integridad de la evidencia, el equipo de primera respuesta debe documentar todas las actividades en los computadores, periféricos, etc.; también proporciona guías para el tratamiento de los equipos cuando estos estén encendidos o apagados.

3. Preservación de la evidencia: al ser la evidencia digital frágil por naturaleza, se requiere un proceso para el empaquetado que incluya elementos como documentado, etiquetado e inventario y uso de paquetes antiestáticos; en cuanto al transporte, considerar que la evidencia digital no debe ser expuesta a campos magnéticos y siempre hacer uso de la cadena de custodia de toda la evidencia trasportada.

2.3.2 RFC 3227 - Directrices para la recopilación de evidencias y su almacenamiento (Brezinski, 2002)

Proporciona las directrices para la recopilación y almacenamiento de evidencia, dentro de las fases y actividades más importantes se destacan:

1. Recopilación de evidencia: se debe considerar listar los sistemas involucrados en el incidente de manera que se cuente con una perspectiva de cuál es la evidencia que debe ser recolectada. Así mismo, considerar elementos como: generar una imagen del sistema lo más precisa posible, documentar cada acción que se ejecute, considerar el orden de volatilidad en la adquisición, iniciar desde lo más volátil (registros y contendidos del cache) al menos volátil (documentos). También proporciona guías de situaciones que se deben evitar, como lo son: apagar el equipo, confiar en la información que proporcionan los comandos del sistema, etc.

2. Preservación de evidencia: se pone especial énfasis en la cadena de custodia y el almacenamiento de información en dispositivos con seguridad demostrada y que permitan control de acceso.

2.3.3 ISO 27037:2012 Guidelines for identification, collection, acquisition, and preservation of digital evidence (ISO, 2012).

1. Identificación. - involucra el reconocimiento y documentación de evidencia digital, se pone énfasis en la consideración del orden de volatilidad de manera que se proteja la evidencia.

2. Recopilación de evidencia. - consiste en remover la evidencia de su origen a laboratorio o sitio seguro. Es importante considerar si el equipo se encuentra encendido o apagado, de manera que se tomen en consideración las actividades a ser ejecutadas y las herramientas a ser usadas.

3. Adquisición. - es realizar una imagen (copia) de los dispositivos que mantienen evidencia digital, se establecen las actividades y herramientas de manera que el proceso sea lo menos intrusivo y finalmente se debe mantener la documentación completa.

4. Preservación. - involucra la salvaguarda de la potencial evidencia digital, la preservación debe mantenerse durante todo el proceso.

Uno de los componentes claves dentro del proceso es la cadena de custodia la cual inicia las actividades de adquisición y/o recopilación.

2.4 Modelo Propuesto

En párrafos anteriores tratamos una serie de estándares para el manejo de la evidencia digital; en este apartado proponemos un modelo para el manejo de evidencia digital, el cual tome en consideración las reglas de evidencia y las actividades más relevantes de los estándares internacionales. Este consta de las siguientes actividades:

1. Identificación: Implica identificar la evidencia potencial a ser recolectada o adquirida, en la cual, sus tareas principales son:

• Efectuar un análisis de riesgos para cada una de las causas probables identificadas, de manera que se determine el impacto y probabilidad de que otros dispositivos y sistemas se encuentren involucrados.

• Establecer los principales objetivos e hipótesis para la investigación.

• Seleccionar las herramientas a ser usadas, tanto de hardware y software.

• Generar una lista de evidencia lógica y física a ser adquirida o recopilada.

2. Fijación fotográfica: Implica realiza varias fotografías de 360 grados del lugar. Se deben fotografiar elementos como: computadores, medios de almacenamientos (USB, discos externos, documentos, etc.), esto permite recrear la escena por los investigadores a posteriori.

3. Adquisición de evidencia volátil: En base al análisis del caso, en la etapa de identificación, es posible determinar si se requiere evidencia no volátil; para lo cual debemos considerar que, si el dispositivo se encuentra encendido por ningún motivo se lo debe apagar, debido a que se perdería la información que se encuentra en la memoria principal. Para realizar la adquisición de la memoria, se requiere acceder al sistema operativo de equipo y proceder a ejecutar herramientas previamente probadas para la adquisición de memoria; si es necesario ejecutar comandos, no utilizar herramientas existentes en el sistema operativo, sino usar herramientas propias como es el caso de líneas de comandos portables; los mismos que deben residir en un dispositivo externo como una USB preparada para estos casos.

4. Adquisición de almacenamiento permanente: Si el dispositivo se encuentra encendido, proceder a apagarlo desconectándolo de la fuente de energía, considerar si el sistema operativo pueda quedar corrupto por este tipo de procedimiento, caso contrario realizar un apagado normal del equipo. Proceder a extraer las unidades de almacenamiento y realizar fijación fotográfica de la unidad (marca, serie, etc.), hacer uso de quipo antiestático de manera que se protejan los dispositivos y proceder a realizar una copia exacta (bit-stream) una vez el dispositivo se encuentre bloqueado para escritura, esto permite preservar la evidencia original. Existen dos métodos de adquisición por los que se puede optar: disco a imagen o disco a disco. Es recomendable usar el primer método debido al aprovechamiento de opciones como la compresión de las imágenes que permite un mejor uso de los dispositivos de destino y de duplicación. Considerar el segundo método únicamente cuando existan errores de hardware del dispositivo de almacenamiento.

Un tema importante a destacar es la existencia de equipos de misión crítica o sistemas de almacenamiento que no son posibles realizar con una copia bit-stream, por lo cual se debe realizar (dependiendo el caso) un tipo de adquisición lógica que captura únicamente los archivos de interés o “sparse” y que se diferencie de la adquisición lógica porqué además adquiere los fragmentos de información borrada (unallocated data).

En la actualidad la mayor parte de herramientas forenses, genera el HASH al mismo tiempo en la que se genera la imagen, por lo que posteriormente se debe calcular el HASH de la imagen realizada y proceder a comparar con el HASH origen, para comprobar la integridad de la misma.

Es importante hacer uso de equipo especializado de hardware y software debidamente probado y el personal entrenado para su manejo.

5. Recopilación de dispositivos: Si el equipo se encuentra apagado, desconecte la alimentación de energía y si tiene batería, retírela, remueva otros cables que se encuentren conectados y etiquételos. Bloquee el botón de encendido para evitar que se encienda de manera accidental.

6. Cadena de custodia: Registra de forma adecuada el manejo y almacenamiento que se da a una pieza de evidencia, este debe contener al menos:

- Fecha y hora
- Ubicación geográfica
- Nombre del cliente/oficina
- Nombre del investigador/consultor que etiqueta
- Nombre de quien realiza la adquisición de la información
- Método de adquisición / recopilación

- Estado en la que se encuentra la evidencia
- Descripción del ítem:

  HASH

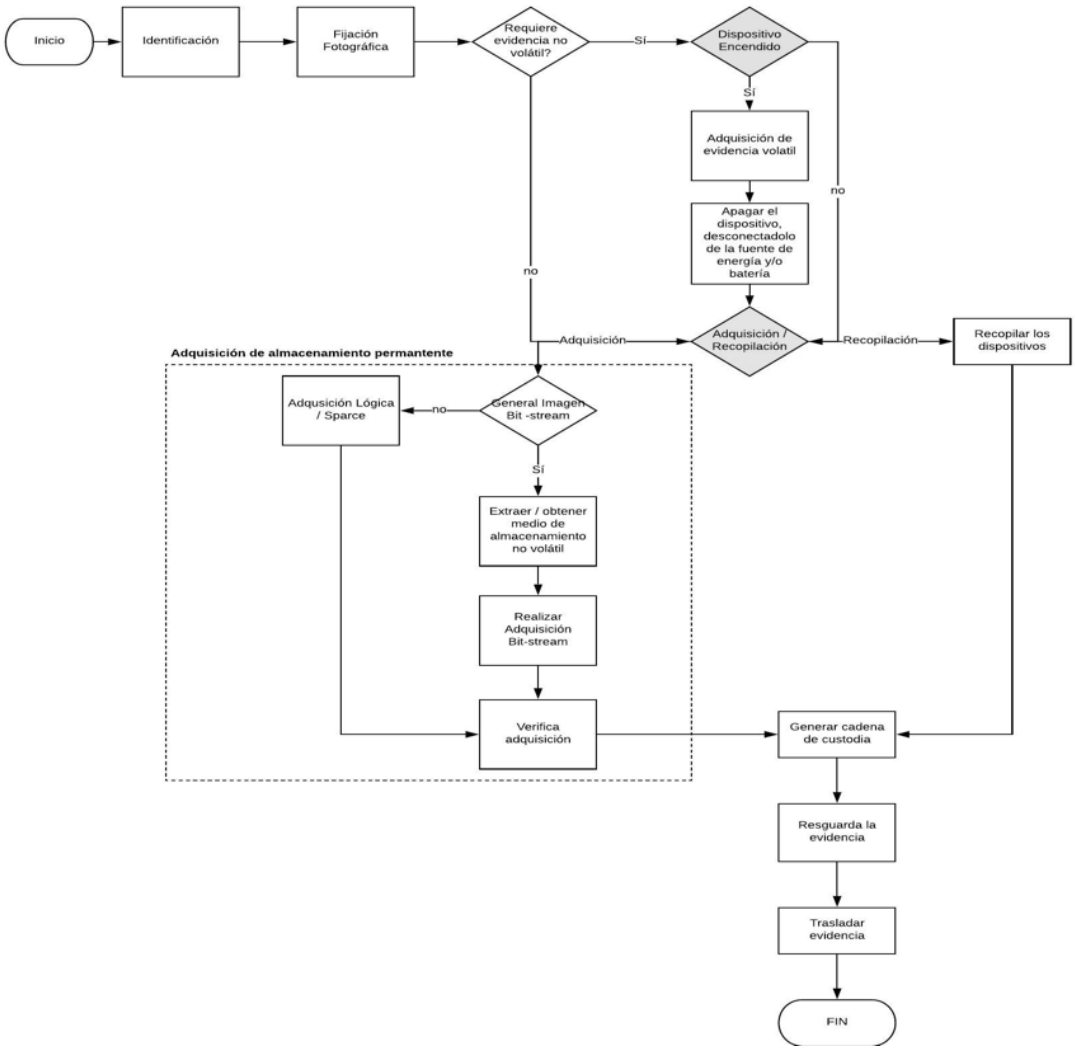
  Identificador (Serial)

  Notas relevantes
- Propósito (peritaje, custodia, traslado, creación imagen, entrega al cliente, destrucción).

7. Resguardar la evidencia: Embalar y sellar la evidencia bajo condiciones adecuadas en función al tipo de evidencia, hacer uso de fundas antiestáticas, contenedores acolchados, etc.; se debe sellar el contenedor, indicando los datos de la persona que realizado dicha actividad.

8. Trasladar la evidencia: Completar la cadena de custodia, indicando: fecha y hora de entrega, nombre, cedula de identidad, firma, nombre y observaciones de quien envía y recibe. Finalmente, proceder a trasladar la evidencia.

Gráfico 1. Modelo propuesto



Fuente y elaboración: El autor

3. Resultados y discusión

La evolución constante de tecnología y el amplio espectro de amenazas requieren un constante desarrollo de procesos para el tratamiento y análisis de la evidencia digital, ante todo, en temas que constituyen un reto para la computacion forense, como son; la computación en la nube, el internet de las cosas, etc.

Cabe mencionar que la evidencia digital puede ser necesaria en diferentes situaciones, como son: procesos judiciales, investigaciones internas, analisis de malware, etc. Los detalles exactos de cada paso pueden variar en base al objetivo específico de lo que se necesite procesar, por ejemplo: las actividades a detalle para realizar la adquisición de un archivo de correo es diferente a las actividades para obtenerlo desde un archivo de log (Archive Logs) de una base de datos.

Por tanto, la evidencia al ser frágil por naturaleza, sin un tratamiento digital adecuado, implica la destrucción de la misma y por ende la imposibilidad de poder presentar en una corte y lo que es talvez más importante, mejorar las medidas de seguridad.

El tratamiento y análisis adecuado de la evidencia trae consigo la mejora de la seguridad de la información entre todos los actores que forman parte de una transacción; es por estas razones, que la red global de pagos SWIFT publicó un conjunto de controles de seguridad para ayudar a los clientes a mejorar la seguridad de la infraestructura.

Las organizaciones con miras a mejorar su proceso de gestión de incidentes de seguridad de la información, requieren prestar atención a elementos tales como:

- Mantener respaldos de sistemas criticos de la organización, la cual debe acompañarse de una política de retención de los mismos.
- Habilitar las opciones de auditoria en estaciones de trabajo, servidores, bases de datos, aplicaciones y componentes de red.
- Usar sistemas para la centralización de logs.
- Usar sistemas para monitorear la integridad de archivos de sistemas y archivos críticos, como pueden ser los archivos de configuración.

Por las razones expuestas, las actividades de adquisición y/o recopilación de evidencia deben intregrarse al proceso de gestión de incidentes, permitiendo un examen (obtención de datos relevantes para el caso) de la evidencia y su correspondiente análisis, el cual debe contar con el respectivo asesoramiento legal, de manera que se usen métodos y técnicas legalmente justificables.

Es de vital importancia mantener un procedimiento para el tratamiento de evidencia digital, el cual debe considerar las mejores prácticas existentes; sin embargo, el mismo debe ser acoplado a la diversa realidad de las empresas y países, con la finalidad de que dicha evidencia tenga valor en un proceso judicial y/o investigación interna.

4. Conclusiones

El tratamiento de la evidencia digital es parte integral de la gestión de incidentes de seguridad, permitiendo conocer la anatomía de los ataques internos y/o externos, de manera que se puedan establecer las medidas corrrectivas y de ser el caso seguir los procesos judiciales pertinentes.

El artículo presenta una perspectiva técnica del tratamiento de la evidencia digital, no es una visión desde el punto de vista de agencias de ley; pretende contribuir como un punto de inicio en el desarrollo de las capacidades en una de las fases de la computación forense; uno de los factores criticos de éxito dentro de este proceso, requiere un trabajo de la mano con los departamentos legales, entes reguladores, policia judicial y la alta dirección de las empresas.

Las organizaciones ya sean públicas o privadas estan expuestas a entidades criminales bien estructuradas, las cuales se centran en buscar aplicaciones de alto valor para encontrar vulnerabilidades y poder explotarlas. Es por esto, que requerimos ahondar esfuerzos en colaborar entre instituciones, con la finalidad de no volver a repetir errores o simplemente reducir el expectro de amenzas.

Por lo expuesto, se requiere un proceso bien estructurado para el tratamiento de evidencia, que permita aprender de los incidentes de seguridad y poder judicializar los mismos; esto, debe venir de la mano con una cooperación internacional eficiente que permitan la protección de los registros.

El Ecuador si bien ha mejorado en su derecho sustantivo de delincuencia cibernetica, el cual se ecuentra en un estado “establecido”, según el informe de ciberseguridad 2016 de la OEA; requiere mejorar elementos que se encuentran en estado “formativo“ tales como: el derecho procesal, investigación jurídica, educación, formación, privacidad y protección de datos, etc.; lo que claramente contribuirá en la lucha contra la ciberdelincuencia.

5. Referencias bibliográficas

Anthony Reyes, J. W. (2007). Cybercrime and Digital Forensics. Syngress Publishing. Inc.

Banco Del Austro, S.A., v. Wells Fargo Bank, 1:2016cv00628 (S.D.N.Y 2016).

Brezinski, K. (2002). RFC 3227 Evidence Collection and Archiving. Obtenido de https://www.ietf.org/rfc/rfc3227.txt

ISO. (2012). ISO 27027:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence.

Justice, U. D. (2008). A Guide for First Responders, Second Edition .

Sheetz, M. (2013). Computer Forensics : An Essential Guide for Accountants, Lawyers, and Managers. John Wiley & Sons.

SINGH, I. (04 de 2018). /www.nirc-icai.org. Obtenido de http://www.nirc-icai.org/BMaterial/Digital%20Forensics%20and%20Invesstigation.pdf

SWEDGE. (04 de 2018). Obtenido de https://en.wikipedia.org/wiki/Scientific_Working_Group_on_Digital_Evidence

Timothy Grance, S. C. (2006). Guide to Integrating Forensic Techniques into Incident Response. Obtenido de https://www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response

Trustwave. (04 de 2018). Global Security Report. Obtenido de https://www2.trustwave.com/rs/815-RFM-693/images/Trustwave_2018-GSR_201803Interactivtok=eyJpIjoiWVdJNE9UY3hZV1kxWVRaayIsInQiOiJjeVBpeWFZZ3BvRnA2eTF6VnZMV0lxK1ZUV1QzZXpmSkVaZmorNFlwSnRYcXZ2WlgyZ0-VuNUFieXQ0YW5zMmxcL1NVbWJGblBJZE5NNmxyT2tEc2M4Tl