Enfoque UTE, V.9-N.1, Mar.2018, pp. 90 - 101
http://ingenieria.ute.edu.ec/enfoqueute/
e-ISSN: 1390-6542 / p-ISSN: 1390-9363

Recibido (Received): 2017/11/23
Aceptado (Accepted): 2018/03/30

Estrategia para responder a incidentes de inseguridad informática ambientado en la legalidad ecuatoriana

(Strategy for responding to computer incidents of insecurity set in Ecuadorian law)

Rodrigo Arturo Proaño Escalante[1], Andrés Fernando Gavilanes Molina[1]

Resumen:
Garantizar la seguridad de la información, los sistemas de información, servicios y redes implica socializar, también conocer cómo responder ante un evento donde se ha vulnerado dicha seguridad informática y cómo gestionar la evidencia digital identificada, fruto de una vulnerabilidad de seguridad informática. El presente trabajo entrega una solución, basada en estándares internacionales y acatando la legalidad ecuatoriana vigente. Los indicios digitales serán identificados en la escena de un incidente informático por parte de los peritos autorizados. La autorización debe señalar lo que motiva, faculta y limita la identificación de pruebas. La fase de obtención de los indicios digitales identificados dependerá de las circunstancias y políticas internas establecidas. La preservación de las pruebas objetivas se la realiza mediante la cadena de custodia y se reportan los resultados verificables, íntegros y confiables. Se aplicó la estrategia descrita previamente como caso de estudio a los incidentes de violación de seguridades lógicas. En este sitio se reconoció, extrajo, custodió e informó acerca de la evidencia digital hallada en el lugar. Durante todo el proceso se implementó la cadena de custodia, la cual garantizó la integridad, confiabilidad de los datos. En cada fase se registró cómo, cuándo, dónde y quién manipuló tanto los indicios digitales como los dispositivos digitales.

Palabras clave: incidente; evidencia digital; seguridad informática; ciberdelito; informática forense.

Abstract:
Assurance the security of information, information systems, services and networks implies socializing, also knowing how to respond to an event where such information security has been violated and how manage the identified digital evidence. The present paper is a solution, based on international standards and complying with the current Law of Ecuador. Digital evidence will be identified at the scene of a computer incident by the authorized persons. The authorization must indicate what motivates, authorizes and limits the identification of evidence. The phase of obtaining the digital evidence identified will depend on the established internal circumstances and policies. The preservation of the objective evidence is carried out through chain of custody, the verifiable, complete and reliable results are reported. The previously described strategy was applied as a case study to the incidents of violation of logical securities. The digital evidence found in the place was recognized, extracted, preserved and informed about. Throughout the process, the chain of custody was implemented, which assurance the integrity and reliability of the data. In each phase it was recorded as, when, where and who manipulated both digital signs and digital devices.

Keywords: informatic security; cybercrime; computer forensics; incident; digital evidence

[1] Universidad Tecnológica Equinoccial, Quito–Ecuador({rodrigo.proano, gmaf1023784} @ute.edu.ec).

1. Introducción

Los incidentes de seguridad informáticos y ciberdelitos se generan, entre otras causas, por una deficiente cultura digital y moral, además de una carente o por lo menos deficiente normativa respecto a la manipulación, transmisión, recuperación y almacenamiento de los datos y evidencias. El desconocimiento u omisión de buenas prácticas incrementa las vulnerabilidades de seguridad. S. Ortiz (2015) en su artículo manifiesta la insuficiencia de profesionales ecuatorianos calificados para la gestión de indicios digitales, lo cual da lugar a la ocurrencia de sesgos inherentes a la profesión. Son algunos de los motivos para que los eventos ilícitos como el robo, fraude, sabotaje y otros delitos cometidos mediante medios electrónicos queden impunes.

El actual Código Orgánico Integral Penal, COIP (2014) no establece un modelo unificado nacional para el actuar del perito informático. Además, el Instituto Nacional de Estadísticas y Censos, INEC en el año 2016 publicó que el 63,8% de los ecuatorianos han utilizado internet en el área urbana (INEC, 2017); es decir, cada vez más personas utilizan dispositivos digitales, formando parte del incremento de incidentes de seguridad informática sin resolver o sin una sanción, generados por una normativa incompleta que no dicta el correcto actuar del perito informático, dicho contexto motivó la presente investigación.

El Servicio Ecuatoriano de Normalización, INEN de acuerdo con las funciones que determina la ley manifiesta que: “la reglamentación técnica comprende la elaboración, adopción y aplicación de reglamentos técnicos necesarios para precautelar los objetivos relacionados con la seguridad, la salud de la vida humana, animal, vegetal, la preservación del ambiente y la protección del consumidor contra prácticas engañosas”. Sin embargo, en el catálogo de normas INEN (2017), aún no se registra reglamentación para el estudio técnico y tecnológico de los indicios digitales competentes y relevantes.

Se publicó un artículo de Solís, F., Pinto, D., & Solís, S. (2017), en la revista Enfoque UTE donde se menciona que, "la seguridad informática cumple un papel muy importante para garantizar la disponibilidad, privacidad e integridad de la información", sin embargo, las políticas o controles de seguridad de la información por sí solos no garantizarán la protección total de la información, los sistemas de información, los servicios o las redes. De acuerdo con ISO/IEC 27035-1 (2016), los controles implementados mitigan los riesgos, pero existe la probabilidad que persistan vulnerabilidades residuales que reducen la efectividad y facilitan la ocurrencia de incidentes de seguridad de la información.

Se han realizado trabajos de investigación ecuatorianos relacionados como una propuesta de diseño de un área informática forense para un equipo de respuestas ante incidentes de seguridad informáticos. En las Conferencias internacionales de sistemas de información y ciencias de la computación, INCISCOS 2017 (International Conference on Information Systems and Computer Science, INCISCOS) se presentó un artículo denominado Guía para reconocer, recoger, extraer, proteger e informar la evidencia digital (Proaño Escalante, R., Gavilanes Molina, A., 2017); justamente este artículo es una extensión del presentado previamente en INCISCOS 2017 y un estudio cualitativo de la relación de las leyes y la pericia informática en el Ecuador (Bolaños Burgos, F., & Gómez Giacoman, C., 2015) los mismos que han servido de base para este trabajo.

Con el fin de proporcionar una ayuda en la gestión de los indicios digitales para que sean considerados como prueba válida, debido a que, se encuentra alineada con las leyes aplicadas en la legislación ecuatoriana y basada en estándares internacionales como: ISO/IEC 27000 (2016) Sistemas de gestión de la seguridad de la información, resumen y vocabulario (Information security management systems Overview and vocabulary), ISO/IEC 27037 (2012) Directrices para la identificación, recolección, adquisición y preservación de la evidencia digital (Guidelines for identification, collection, acquisition and preservation of digital evidence), ISO/IEC 30121 (2015) Gobernanza del marco digital de riesgo forense (Governance of digital forensic risk framework), ISO/IEC

27035-1 (2016) Gestión de incidentes de seguridad de la información (Information security incident management).

El cumplir con un adecuado procedimiento y contar con personal calificado, asegura la credibilidad, autenticidad e integridad de la investigación realizada. La metodología propuesta consta de cinco fases que son: identificar, obtener, extraer, custodiar e informar evidencia digital relevante, suficiente y confiable. Es decir, se enfoca en las primeras acciones a realizar después de un incidente de seguridad informática, con especial atención a la evidencia digital debido a que es un elemento clave durante todo el proceso de peritaje informático.

Este procedimiento se aplicó en los laboratorios de computación de una institución de educación superior, en un caso práctico de estudio orientado a incidentes de seguridad lógica, enmarcado en la actual normativa legal ecuatoriana. Cada una de las actividades realizadas durante la operación de la presente metodología fue debidamente documentada a detalle. Se identificó evidencia digital con conexión a red, discos duros, discos sólidos, cámaras de video y computadores; cabe notar que los dispositivos se encontraban encendidos. Inclusive se conversó asertivamente con las personas a cargo del lugar, con el fin de recabar información relevante en cada caso.

2. Metodología

Basado en los cinco procesos de la metodología PMI (Project Management Institute, PMI), tomada del PMBOK (2013): Guía para la dirección de proyectos; se establecieron los grupos de procesos PMI para gestionar evidencia digital al existir un incidente de seguridad informático, los mismos que se muestran en la *Tabla 1*, en la cual se puede observar los distintos procesos y actividades relacionados con el peritaje informático.

Las acciones a ejecutar son reproducibles y son aplicables en el inicio de un incidente, en consecuencia, la prioridad de las acciones está dada por el estado del dispositivo involucrado, ya sea que esté apagado o encendido. En la *Figura 1*, se muestran las cinco fases establecidas para la intervención de los indicios digitales, fundamentadas en las consideraciones definidas por ISO/IEC 27037 (2012), Directrices para la identificación, recolección, adquisición y preservación de la evidencia digital (Guidelines for identification, collection, acquisition and preservation of digital evidence), Ayers, Brothers y Jansen (2014) e ISO/IEC 27000 (2016).

2.1. Fase 1: identificar

Según Dykstra y Riehl (2012), en el incidente se puede encontrar evidencia digital tangible e intangible, incluso puede estar oculta o visible; razón por la cual, se establece una prioridad para la obtención de indicios y se toman en cuenta su volatilidad y criticidad. Los medios de almacenamiento y/o dispositivos de procesamiento que contengan datos asociados al hecho, deberán ser identificados, reconocidos y documentados por parte del personal técnico autorizado. La legislación informática ecuatoriana cuenta con un conjunto de ordenamientos jurídicos establecidos con el fin de regular el tratamiento de la información.

En el estándar ISO/IEC 27035-1 (2016): Gestión de incidentes de seguridad de la información (Information security incident management), se menciona la necesidad que el técnico a cargo documente todo su proceder, por lo cual es importante comenzar con la documentación desde el registro de la persona o sistema que reportó o encontró el incidente de seguridad informática. Según ISO/IEC 27037 (2012), recomienda tener cuidado con las bombas lógicas que destruyen, estropean o modifican datos si se desconecta o se accede de forma incontrolada, así como identificar el posible acceso remoto a cualquier dispositivo digital, y si dicho acceso representa una amenaza para la

integridad probatoria, también hay que analizar si los datos y/o equipos están dañados o comprometidos.

Tabla 1. Grupo de procesos PMI, ambientados a la dirección de peritaje informático

GRUPOS DE PROCESOS PARA LA OBTENCIÓN DE EVIDENCIA DIGITAL					
ACTIVIDAD	INICIO	PLANIFICACIÓN	EJECUCIÓN	MONITOREO Y CONTROL	CIERRE
Peritaje Informático	Documento habilitante	Recopilar requisitos	Gestionar el trabajo	Control de cambios	Cerrar fase
		Definir alcance		Validar alcance	
		Crear EDT/WBS		Controlar alcance	
		Definir y secuenciar las actividades		Control de cronograma	
		Desarrollar el cronograma	Adquirir equipo		
			Dirigir equipo		
			Gestionar comunicaciones	Controlar las comunicaciones	
		Estimar recursos	Efectuar adquisiciones	Controlar los costos	Cerrar compras
		Presupuesto		Controlar adquisiciones	
		Gestión de la calidad	Realizar aseguramiento de la calidad	Controlar la calidad	
	Análisis de interesados	Identificar los riesgos	Gestionar la participación de los involucrados	Controlar los riesgos	
		Análisis cualitativo del riesgo		Controlar la participación de los interesados	
		Análisis cuantitativo del riesgo			

2.2. Fase 2: obtener

Una vez identificados los elementos verificables, de acuerdo con las circunstancias, costo y tiempo se decide entre recoger o extraer, por lo cual se incluyen las razones por las cuales no se recogió cierto elemento identificado. El proceso de recoger evidencia digital es retirar la evidencia desde su lugar de origen hacia un ambiente controlado para su posterior extracción y análisis.

En esta fase se documentan todas las acciones u omisiones tomadas, incluso se obtiene cualquier material como apuntes, contraseñas escritas en papel, conectores entre otros. Es importante recordar que, el seleccionar o utilizar una herramienta inadecuadamente para recoger o extraer la evidencia digital, puede producir la pérdida parcial o total de la misma, por tal razón, ISO/IEC 27037 (2012) considera relevante evaluar sistemáticamente los riesgos y su impacto.

La elección de las herramientas y técnicas está determina por: el estado del sistema, ya sea apagado o encendido; existencia de cifrado, como contraseñas o clave alojados en RAM, en fichas externas, chips; criticidad del sistema y requisitos legales; espacio de disco requerido para el almacenamiento y la disponibilidad de personal, limitaciones de tiempo. Al recolectar el material es necesario conocer la probabilidad de

infringir la Ley u ocasionar daños psicológico, emocional o físico; se debe recordar asegurar la escena del incidente y detectar en el área elementos potenciales de riesgo.

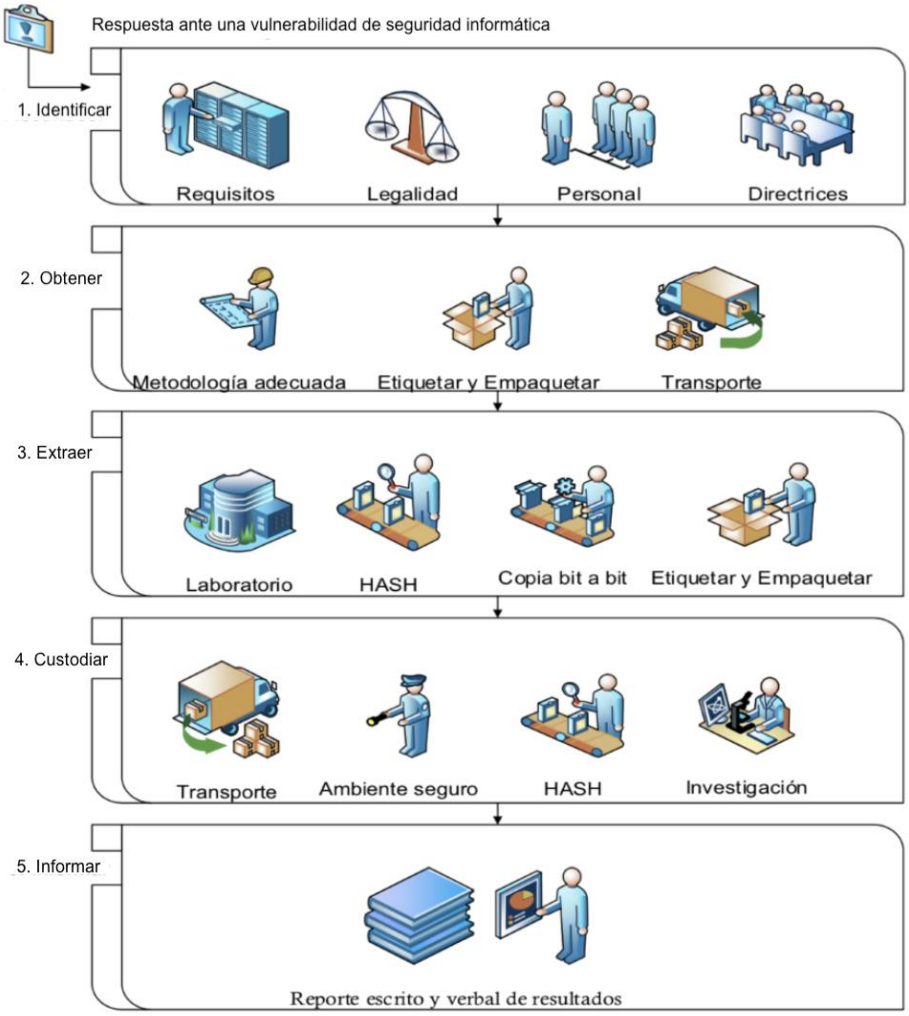

Figura 1. Manipulación de la evidencia digital en primera instancia

2.3. Fase 3: extraer

La extracción consiste en, sin introducir cambios, generar una copia *bit* a *bit* de la evidencia digital relevante; se deben documentar los métodos, herramientas y actividades utilizadas. En la publicación especial del NIST 800-175B (2016): Estándares criptográficos en el gobierno federal: mecanismos criptográficos (NIST Special Publication 800-175B Cryptographic Standards in the Federal Government: Cryptographic Mechanisms) y en ISO/IEC 27037 (2012) se menciona que la copia como su original deben ser comprobados con una función de verificación (*hash*) aceptable. El resultado *hash* del original y la copia debe coincidir para validar su originalidad.

Al momento de extraer, recordar las características de las pruebas digitales establecidas por ISO/IEC 27037 (2012), las pruebas digitales deben cumplir con cuatro características, que son: Justificación (Justificability), Auditabilidad (Auditability), Repetibilidad (Repeatability) y Reproducibilidad (Reproducibility). La extracción de evidencia digital está supeditada por factores ambientales como: recursos financieros, tiempo y particularidades de los sistemas críticos. Cuando no sea factible y/o permisible, se extrae de manera lógica, esto es justificar y seleccionar de manera específica ciertos tipos de datos, archivos o ubicaciones.

Cabe mencionar que, los principios sustanciales de la evidencia digital, de acuerdo con ISO/IEC 27037 (2012) son: Relevancia (Relevance), Confiabilidad (Reliability) y Suficiencia (Sufficiency). Tanto las características como los principios de la evidencia digital deberán ser cumplidos por parte del personal técnico autorizado.

2.4. Fase 4: custodiar

La integridad de la evidencia digital puede ser alterada, divulgada y/o destruida, lo cual provoca resultados incoherentes. De existir varios interesados en la problemática, la intervención debe ser coordinada con los demás recolectores de evidencia.

Una cadena de custodia es documentar completa y cronológicamente todas las acciones establecidas por parte del técnico a cargo, desde el instante que se identifican, obtienen, extraen y cómo se protegen las pruebas digitales, también el estado y ubicación de la misma. Custodiar proporciona trazabilidad, integridad y autenticidad de los procesos relacionados con el tratamiento de las pruebas digitales.

Este proceso preserva la integridad y autenticidad de los elementos probatorios hallados e instrumentos empleados desde su identificación hasta el fin de la cadena de custodia. Esta fase protege, la intromisión de entes no autorizados o malintencionados, el daño consciente o inconsciente, así mismo cuida del desgaste, alteraciones, pérdida de datos. Siempre la vida de las personas será lo más importante, por ende, es pertinente evaluar el riesgo de las personas presentes en la zona del incidente.

En ISO/IEC 27037(2016) se recomienda, si es posible, aislar la zona del incidente de los espectadores y evaluar el riesgo tomando en cuenta la hora, inseguridad, daños a la integridad física, inclusive prever, si existen o no, armas, agresividad, observar las afectaciones térmicas, polvo, grasa, contaminantes químicos que generan óxido, condensación de humedad, emisiones electromagnéticas y estáticas.

2.5. Fase 5: informar

Consiste en consolidar a través de un reporte escrito y verbal, con argumentos, la relevancia y suficiencia de las decisiones u omisiones, así como reportar los resultados. En el informe se resalta la importancia de conocer cuál es la evidencia, cuándo y cómo se la obtuvo, quién y por qué dicha persona la manipuló, además desde dónde fue transportada y el sitio en dónde se resguardó.

El informe deberá ser presentado de manera escrita y verbal en los plazos señalados, de ser el caso, aclarar o ampliar los mismos.

3. Resultados

El día viernes 03 de junio de 2017 a partir de las 16:00 pm, se aplicó la estrategia para responder a un incidente reportado, como caso de estudio a los incidentes de violación de seguridades lógicas. A continuación, se describen los resultados de cada fase.

3.1. Fase 1: identificar

Se tomaron en cuenta las reglas generales de la pericia, mencionadas en el artículo 511 del COIP. Tras haber cumplido con la parte legal se procedió a la búsqueda, identificación y documentación de la evidencia digital relevante en los laboratorios de computación. Además, se cumplió el trámite reglamentario establecido en el artículo 478, literal a) del Código Orgánico Integral Penal, COIP (2014) vigente en la República ecuatoriana, en donde se manifiesta lo siguiente: “los registros de personas u objetos requerirán autorización de la persona afectada o de orden judicial motivada y limitada, al lugar autorizado”.

En el caso de estudio se reconoció todo tipo de información adicional que aporte a la investigación. En la zona del incidente se buscaron materiales como notas adhesivas, diarios, papeles, informes técnicos, computadores, manuales de *hardware* y *software* con detalles sobre los dispositivos (contraseñas, PIN) que se relacionen con el incidente y recordar que estos elementos no siempre se encuentran de manera obvia.

Se empleó el procedimiento para levantar evidencia digital conectada a una red de datos. En esta parte es sumamente importante etiquetar la evidencia. Cabe mencionar que las etiquetas asignadas para los dispositivos identificados en el incidente registran datos como son el identificador institucional del laboratorio y computador, también un código del dispositivo involucrado, como se muestra en la *Figura 2*.

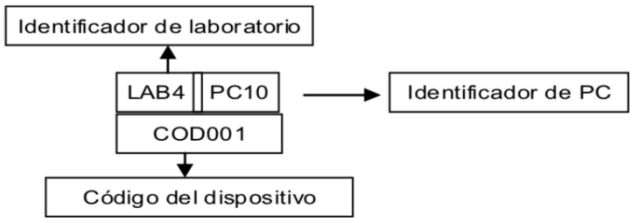

Figura 2. Etiqueta de hardware utilizada.

Para la etiqueta del software se registró la hora, día, mes, año y tipo como se muestra en la *Figura 3*.

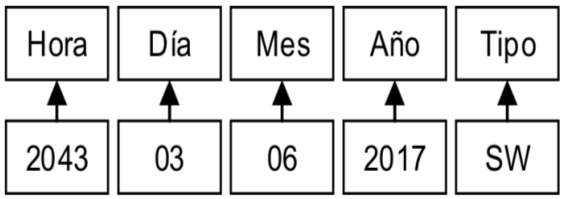

Figura 3. Etiqueta de software utilizada.

3.2. Fase 2: obtener

Una vez detectada la zona del incidente, se delimitó, aseguró y controló el acceso al área que contenía los elementos involucrados como cables, componentes electrónicos y digitales, evitar en lo posible modificar su condición original. Se responsabilizó el cuidado del sitio al personal de seguridad de la institución educativa, quienes vigilaron durante todo el proceso.

Los dispositivos digitales al momento de realizar la recopilación se encontraban en estado encendido, sobre esta situación se seleccionaron y utilizaron herramientas para cumplir con esta fase, respetando las normativas institucionales. Por tal motivo, no se pudo remover los dispositivos digitales de su ubicación original debido a que las políticas internas de la institución educativa no lo permiten.

Como principio básico, si un dispositivo se encuentra encendido no es conveniente apagarlo ya que se corre el riesgo de destruir mucha evidencia relevante imposible de recuperarse posteriormente.

Por ende, fue necesario crear un ambiente controlado, donde no se alteren las condiciones dentro de la zona de los laboratorios de computación de la institución de educación superior, para proceder con la siguiente fase que es la extracción de evidencia digital. Conjuntamente se documentó todo el procedimiento llevado a cabo, así como también se empaquetaron los elementos relacionados con el incidente como contraseñas escritas en papel, memorias USB, CD con videos de seguridad y se identificó su transporte.

3.3. Fase 3: extraer

En esta fase, se realizó el estudio de la evidencia mediante herramientas de *software* elegidas de forma tal que permitan realizar el volcado de memoria, clonación *bit* a *bit* de los datos, función de verificación y comparación. Para el caso de estudio se analizaron computadores de escritorio. Las herramientas de *software*, la versión, el tipo de licencia así como una descripción para la cual fueron utilizadas se muestran en la *Tabla 2*.

Tabla 2. Herramientas de *software* utilizadas

Herramienta	Versión	Tipo	Descripción
Windows	10 Pro	Pago	Sistema Operativo
Windows	8.1	Pago	Sistema Operativo
Internet Explorer	11	Gratuita	Navegador
Mozilla Firefox	49.0.1	Gratuita	Navegador
Wireshark	2.2.7	Gratuita	Captura y analiza paquetes de red
QuickHash Windows	2.6.9.2	Gratuita	Hash de datos
Izarc	4.2	Gratuita	Descomprimir y cifrar archivos
FTK Imager Lite	3.1.1	Gratuita	Herramienta para peritaje informático
Network IP scanner	1.6	Gratuita	Escaneo de red
Microsoft Office	2013	Pago	Ofimática

Es pertinente aclarar que las herramientas, métodos y técnicas utilizadas obedecen al tipo de incidente identificado.

En otras palabras, se analizó el riesgo e impacto de los equipos necesarios, también el nivel de volatilidad de los datos, priorizando los datos más volátiles de acuerdo con su relevancia y valor. También se analizó la información relacionada con la evidencia digital. Luego se evaluó y cumplió con los requisitos de la evidencia digital establecidos por ISO/IEC 27037 (2012) y por el COIP (2014), que son relevancia o pertinencia, confiabilidad y suficiencia.

Al momento de la intervención no existió una limitación en cuanto al análisis de los datos almacenados en los equipos involucrados. No obstante, el tamaño de almacenamiento del sistema era demasiado grande para crear una copia completa del mismo, a más de existir datos irrelevantes, por tal razón la extracción de las pruebas se realizó de manera lógica, lo cual significó que se identificaron y obtuvieron tan solo las carpetas, archivos y otros datos relevantes para el caso investigado.

3.4. Fase 4: custodiar

Se preservaron los elementos probatorios en todo el procedimiento. En esta fase se cumplió con el artículo 456 del COIP (2014), donde se establece que: “la cadena de custodia inicia en el lugar donde se obtiene, encuentra o recauda el elemento de prueba y finaliza por orden de la autoridad competente”. Se identificaron las personas involucradas en la cadena de custodia. De la misma forma se identificó tanto a quien reportó el incidente como quien lo atendió.

Se encontró evidencia digital relevante. Además, se registró detalladamente la obtención de los elementos de convicción y su transporte. Se generó una bitácora del dispositivo afectado que en este caso fue un computador personal. Toda la información encontrada se registra adecuadamente para una evaluación posterior.

3.5. Fase 5: informar

El procedimiento que se utilizó, cumple con lo establecido en los artículos 482, 456, 480, 478 del COIP (2014). Se aplicó la estrategia propuesta y se identificaron como objetivos: identificar, obtener, extraer, preservar e informar la evidencia digital relevante

hallada. Se empleó la herramienta “AccessData FTK Imager” versión 3.1.1, la cual permite hacer un análisis rápido de la evidencia encontrada. La prueba digital obtenida tiene la etiqueta "174303062017SW".

Para verificar la integridad y autenticidad de los datos se utilizó la herramienta “QuickHash” versión 2.6.9.2. en la cual, se ejecutó y comparó exitosamente con el algoritmo SHA256. El algoritmo de verificación utilizado no presentó colisiones y su procesamiento fue eficiente y generó un resultado satisfactorio. Se protegió la integridad y autenticidad de los datos durante todo el proceso, los mismos que fueron comprobados con funciones de verificación SHA256 y SHA1. La fase de traslado de las pruebas se realizó sin ningún inconveniente.

Luego, con la herramienta “AccessData FTK”, se creó una copia *bit* a *bit* de las pruebas obtenidas con su respectiva función de autentificación. La etiqueta de identificación de la copia es “202908062017SW”.

Se revisaron los procesos en ejecución y se encontró “llscv.exe”. Dicho proceso estaba guardando todo lo digitado desde teclado en el archivo plano “KeyStroke1.html”; es decir, es un “Keylogger” (A.Solairaj et al., 2016). De esta forma se obtenían de manera oculta claves de acceso a redes sociales y correos para luego suplantar y alterar la identidad personal del propietario de las credenciales.

4. Discusión

Se utilizó satisfactoriamente la guía metodológica para la obtención de la evidencia digital relevante y suficiente, sin comprometer la confidencialidad e integridad de las pruebas obtenidas. En ISO/IEC 27037 (2012) se menciona que la cadena de custodia juega un rol importante en la investigación del incidente, incluso manifiesta que se debe conocer a detalle cada paso que se dio en el manejo de las pruebas digitales, por lo tanto, para brindar confidencialidad y credibilidad del proceso se implementó una cadena de custodia limpia y sin actos negligentes. Así se cumplió con los requisitos normativos vigentes en la República del Ecuador, así como con los reglamentos internos de la institución educativa.

Cabe mencionar que en el proceso se involucraron 16 cámaras de un total de 48 cámaras de video vigilancia instaladas en la zona del incidente detectado como parte del proceso de obtención de evidencia, esto es importante tomar en cuenta ya que al cabo de un mes comienza la sobrescritura del espacio de almacenamiento del DVR con lo cual se podrían perder evidencias significativas.

Las herramientas “QuickHash” y “AccessData FTK Imager” fueron de gran ayuda, ya que la primera permite con algoritmos criptográficos SHA128, SHA256, SHA512, verificar, comparar y encriptar archivos, mientras que la segunda permite crear imágenes forenses de cualquier dispositivo físico o lógico con función de verificación MD5 y SHA1, entre otras funcionalidades inherentes al peritaje informático.

A.Solairaj, S.C.Prabanand, J.Mathalairaj, C.Prathap y L.S.Vignesh (2016) concluyen que los programas “KeyLogger”, supervisan todas las actividades del usuario en la computadora. Los mismos roban la información confidencial y se ejecutan completamente en modo sigilo. Una vez instalado en un equipo, no se muestra ni en los íconos de inicio ni en ningún otro lugar del equipo que se está supervisando. Además, afirman que los “Keylogger” representan una gran amenaza para la privacidad y la seguridad del usuario. Dicha afirmación es real, ya que este tipo de *software* malicioso se obtuvo como evidencia digital relevante en las computadoras involucradas en el incidente investigado.

Es oportuno mencionar que la detección de “Keyloggers” es difícil porque se ejecutan en modo oculto, sin embargo, existen técnicas que permiten analizar la privacidad y la seguridad del usuario. Se pueden detectar mediante técnicas “Anti-Hook” o “HoneyID” para detección de *spyware*, detección de *bot*, acceso seguro a cuentas protegidas por contraseña y algoritmos de células dendríticas (A.Solairaj, S.C.Prabanand, J.Mathalairaj, C.Prathap y L.S.Vignesh, 2016).

En resumen, las herramientas utilizadas fueron útiles. El uso de este procedimiento, brinda confiabilidad a las pruebas digitales halladas en dispositivos digitales conectados a una red de datos, de tal suerte que, puedan ser presentadas en el ámbito jurídico.

En la Ley de Comercio Electrónico, Firmas y Mensajes de Datos (2002) se considera necesario “impulsar el acceso de la población a los servicios electrónicos que se generan por y a través de diferentes medios electrónicos”, de tal manera que se permita el desarrollo del comercio, la educación y la cultura.

Sin embargo, la capacidad de crecimiento de una correcta cultura digital se obstaculiza o altera cuando el acceso a los servicios electrónicos disponibles es inseguro, es decir inobservancia de estándares, procedimientos, buenas prácticas y herramientas fundamentadas por la normativa ecuatoriana vigente.

5. Conclusiones y recomendaciones

Se actuó dentro del marco legal vigente en el Ecuador, según los artículos 456, 478, 482 y 500 del COIP (2014), los cuales detallan el procedimiento forense.

Cada estándar internacional publicado, debe ser acondicionado a la realidad de cada actividad técnica, sopesando el entorno administrativo en el cual se desenvuelve.

Se obtuvieron pruebas digitales previo inventario detallado de los elementos de convicción. No se realizó embalaje ni traslado, debido a que no lo permite la normativa de la institución educativa.

Se atendió, investigó y resolvió el incidente de inseguridad, encontrándose como evidencia un proceso oculto “llsvc.exe”.

Se cumplió con la prioridad de la evidencia digital volátil establecida por ISO/IEC 27037(2012).

Se verificó la autenticidad de las pruebas obtenidas con la función de verificación SHA256, mientras que para la preservación se usó el algoritmo SHA1, ambas por poseer características como son bajos tiempos de procesamiento y resistencia a colisión.

Se manipuló la prueba digital sin comprometerla y se evitó un mal manejo de la evidencia digital, la cual fue un elemento relevante, pertinente y suficiente.

Se usaron estándares, buenas prácticas y documentación de procedimientos, los cuales aseguraron integridad y confiabilidad del peritaje informático a través de las fases propuestas que son: reconocer, recoger, extraer, proteger e informar pruebas suficientes y relevantes, para obtener así resultados detectables, ubicables y trazables.

La metodología aplicada, garantizó que la evidencia digital seleccionada sea auténtica e íntegra, incluso que la muestra obtenida pueda ser utilizada para defenderse o reclamar justicia.

La guía propuesta puede ayudar al intercambio de evidencia digital entre distintas jurisdicciones, con lo cual se superan limitantes regionales o de un determinado país a través del cual se puede procesar evidencia digital válida en casos de litigio o controversia.

Para verificar un indicio digital se necesita tanto el original como la copia para poder compararlos con la función de verificación (hash) aceptable, caso contrario existiría sesgo profesional.

Como trabajos futuros se prevé incluir recomendaciones para la manipulación de Circuitos Cerrados de Televisión, CCTV, y realizar una evaluación de casos donde la evidencia se encuentra en ambientes virtualizados (Cloud Computing).

La institución educativa de educación superior brindó las facilidades en la aplicación de esta metodología en sus instalaciones, cuyo nombre no podemos publicar por acuerdos de confidencialidad.

Bibliografía

A.Solairaj, S.C.Prabanand, J.Mathalairaj, C.Prathap y L.S.Vignesh. (2016). “Keyloggers software detection techniques”. *Intelligent Systems and Control* (ISCO), 10th International Conference on, Coimbatore, 2016.

AccessData FTK Imager. (2016). *FTK IMAGER VERSION 3.4.3*. Obtenido de: https://accessdata.com/product-download/ftk-imager-version-3.4.3

Ayers, R., Brothers, S., & Jansen, W. (2014). *NIST Special Publication 800-101 Guidelines on Mobile Device*. Obtenido de National Institute of Standards and Technology: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf

Bolaños Burgos, F., & Gómez Giacoman, C. (2015). Estudio cualitativo de las leyes y la pericia informática en el Ecuador. *ReCIBE Revista electrónica de computación informática biomedicina y electrónica*, 1 a 36.

Barker, E. (2016). *NIST Special Publication 800-175B NIST Special Publication 800-175B Cryptographic Standards in the Federal Government:Cryptographic Mechanisms.* Obtenido de National Institute of Standards and Technology: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175B.pdf

Catálogo de normas INEN. (2017). *Servicio Ecuatoriano de Normalización INEN*. Obtenido de http://apps.normalizacion.gob.ec/descarga/

Código Orgánico Integral Penal. (2014). *Código Orgánico Integral Penal*. Quito: Gráficas Ayerve C.A.

Grother, P., Salamon, W., & Chandramouli, R. (2013). *NIST Special Publication 800-76-2 Biometric Specifications for Personal Identity Verification*. Obtenido de National Institute of Standards and Technology: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-76-2.pdf

Hash Project Webmaster. (2015). *SHA-3 STANDARDIZATION*. Obtenido de National Institute of Standards and Technology: http://csrc.nist.gov/groups/ST/hash/sha-3/sha-3_standardization.html

HirensBootCD. (2016). *Hirens Boot CD*. Obtenido de Testing, Backup, Recovery, Password Tools, MiniWindows XP, Partition Tools: http://www.hirensbootcd.org/

ISO/IEC 27000. (2016*). Information technology — Security techniques — Information security management systems — Overview and vocabulary*. Obtenido de Online Browsing Platform (OBP): https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

ISO/IEC 27035-1. (2016). *Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*. Obtenido de Online Browsing Platform (OBP): https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-1:ed-1:v1:en

ISO/IEC 27035-2. (2016). *Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*. Obtenido de Online Browsing Platform (OBP): https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-2:ed-1:v1:en

ISO/IEC 27037. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*. Obtenido de Online Browsing Platform (OBP): https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en

ISO/IEC 30121. (2015). *Information technology — Governance of digital forensic risk framework*. Obtenido de Online Browsing Platform (OBP): https://www.iso.org/obp/ui/#iso:std:iso-iec:30121:ed-1:v1:en

J. Dykstra and D. Riehl. (2012). Forensic Collection of Electronic Evidence from Infrastructure-as-a-Service Cloud Computing, *Richmond Journal of Law & Technology*, vol. XIX, no 1, p. 47, 2012.

Kent, K., & Suzanne, C. (2016). *NIST Special Publication 800-86 Guide to integrating forensic techniques into incident response*. Obtenido de Computer Security Division: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Ley No 2002-67. (2002). *LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS* Ley No. 2002-67. Obtenido de Registro Oficial 557: http://www.arcotel.gob.ec/wp- content/uploads/2015/12/ley-comercio-electronico-firmas-electronicas-y- mensaje-de-datos.pdf

Ortiz, S. (15 de abril de 2015). El Comercio. *49 peritos informáticos rastrean a las cibermafias*.

Plan Nacional del Buen Vivir. (2017). *Objetivo 11: Asegurar la soberanía y eficiencia de los sectores estratégicos para la transformación industrial y tecnológica*. Obtenido de http://www.buenvivir.gob.ec/objetivo-11.- asegurar-la-soberania-y-eficiencia-de-los-sectores-estrategicos-para-la- transformacion-industrial-y-tecnologica#tabs3

Proaño Escalante, R., Gavilanes Molina, A. (2017). Guía para reconocer, recoger, extraer, proteger e informar la evidencia digital. *INCISCOS 2017*.

Proaño Escalante, R., Saguay Chafla, C., Jácome Canchig, S., & Sandoval Zambrano, F. (2017). Sistemas basados en conocimiento como herramienta de ayuda en la auditoría de sistemas de información. *Enfoque UTE*, 8(1), pp. 148-159. doi:https://doi.org/10.29019/enfoqueute.v8n1.122

Project Management Institute. (2013). *Guía del PMBOK*. Obtenido de Guía de los fundamentos para la dirección de proyectos: https://www.gob.mx/cms/uploads/attachment/file/79535/PMBOK_5ta_Edicio n_Espanol__1_.pdf

Solís, F., Pinto, D., & Solís, S. (2017). Seguridad de la información en el intercambio de datos entre dispositivos móviles con sistema Android utilizando el método de encriptación RSA. *Enfoque UTE*, 8(1), pp. 160-171. doi:https://doi.org/10.29019/enfoqueute.v8n1.123

Tedtechnology. (2017). *sourceforge.net.* Obtenido de Quick Hash GUI: https://sourceforge.net/projects/quickhash/