REALITIES OF A COMPUTER CRIME IN BOYACÁ

Article Information:

Received: October 8, 2013
Accepted: December 13, 2013

Keywords: Security Incidents, Forensic computing, Chain of custody, Collection techniques, Validating digital evidence.

Abstract: The level of training of both: professionals in information security and institutions of governmental nature to address crimes against digital information, are the objectives of the present article, which involves a discipline called forensic computing; their uses, methods for procedures and use of methodologies are in accordance to current legislation and international standards such as the norm ISO/IEC 27037 - 2012, which refers to information technology, security techniques and Guidelines for identification, collection, acquisition, and preservation of digital evidence. The document sets the process exhaustively as well as the elements of hardware and software used for this kind of studies; methods of obtaining data, and the true value of developing and maintaining a chain of custody with the collected evidences.

REALIDADES DE UN DELITO INFORMÁTICO EN BOYACÁ

Rocío del Pilar Avella Pinzón[1], Esp., Manuel Salvador Gil Gamboa[2], Esp., John A. Bohada[3], Ph.D.

Grupo de investigación MUISCA, Facultad de Ingeniería, Especialización en Seguridad de la Información, Fundación Universitaria Juan de Castellanos, Tunja, Colombia.

[1]pilar.avella@gmail.com, [2]manugil17@gmail.com, [3]jbohada@jdc.edu.co

Información del artículo:

Recibido: 8 de octubre de 2013
Aceptado: 13 de diciembre de 2013

Palabras Claves: Incidentes de seguridad, Informática Forense, Cadena de custodia, Técnicas de recolección, Validación evidencia digital.

Resumen: El nivel de preparación que hay, tanto en profesionales de la seguridad de la información, como en las instituciones de carácter gubernamental para hacer frente a delitos contra la información digital, son los objetivos de este artículo, donde interviene una disciplina denominada informática forense, sus campos de aplicación, métodos para realizar procedimientos y uso de metodologías acordes con la legislación vigente y estándares internacionales como la norma ISO/IEC 27037 - 2012, la cual hace referencia a (Tecnología de la información, técnicas de seguridad, guías para la identificación, recolección, adquisición y preservación de la evidencia digital). En ese sentido, el documento expone el proceso de manera exhaustiva, así como los elementos de hardware y software utilizados para este tipo de estudios, métodos para la obtención de datos, y el valor de elaborar y mantener una cadena de custodia con las evidencias recogidas.

1. INTRODUCCIÓN

Dados los grandes avances tecnológicos especialmente en el campo de la computación y las telecomunicaciones, donde a diario, miles de datos son generados y guardados por los usuarios en todo tipo de dispositivos de almacenamiento físicos o virtuales, hace que estos elementos tecnológicos se conviertan en escenarios ideales para personas que disfrutan o se lucran obteniendo ilegalmente información de todo tipo, ya sea esta personal o de carácter confidencial para las empresas; instituciones donde la información juega un papel relevante y se transforma en un activo muy preciado y digno de extrema protección, dado que un evento de seguridad, los deja expuestos a perjuicios tanto económicos como de imagen y pueden llegar a afectar en gran medida la productividad de dichas compañías o personas.

Por lo descrito anteriormente, se hace indispensable determinar la forma correcta como se debe adelantar un proceso investigativo, qué herramientas de hardware y software son indispensables para lograr este cometido y cómo ceñirse a una metodología estandarizada nacional e internacionalmente, que permita de forma profesional examinar los lugares donde se hubiese cometido un ilícito y, de esta manera, estar en la capacidad de rastrear dispositivos computacionales o elementos de las telecomunicaciones que fueron usados por los intrusos para penetrar arbitrariamente la privacidad individual o de una organización. Es allí, en estos espacios, donde el investigador requiere actuar sobre acciones específicas de manera correcta, en aras de iniciar y construir sólidamente un caso de carácter judicial, conociendo de antemano qué tipo de métodos son válidos para la recolección de evidencia digital ante un incidente de seguridad y lograr llevar a cabo una secuencia de acciones bien estructuradas que le den la facultad de emitir de manera sólida un concepto idóneo e imparcial, como profesional apto en las técnicas de peritaje forense, manejo y análisis de evidencia digital, aportando positivamente a los procesos de investigación.

De esta manera se busca llevar a cabo una revisión de carácter regional con el fin de tener conocimiento si en el departamento de Boyacá, existe el personal y las instituciones idóneas, capacitadas para hacer frente a hechos de este tipo, a su vez, verificar el nivel de formación que las instituciones de educación superior y técnica brindan en el campo de la seguridad de la información. Tras realizar las anteriores indagaciones, se espera obtener una clara visión de la realidad que permita fortalecer la proyección académica teórico-práctica con énfasis interdisciplinario, donde los diferentes actores policivos, judiciales, administrativos y técnicos sean capacitados para atender a nivel local las necesidades relacionadas con los delitos que se cometen, favoreciendo la actualización permanente ante las realidades emergentes, frente a los delitos contra la información digital y sus medios de comunicación.

Este tema de reflexión, identifica los estándares RFC 3227 y la norma ISO/IEC 27037:2012, reconocidos y aceptados internacionalmente, dado que para nuestro caso temático, pone a disposición una completa y bien detallada guía de lo que se debe hacer ante un incidente de seguridad.

La norma ISO/IEC 27037:2012 [1] proporciona orientaciones sobre mejores prácticas en la identificación, adquisición y preservación de evidencias digitales potenciales que permitan aprovechar su valor probatorio. Se orienta a su uso en investigaciones forenses digitales, destinadas al esclarecimiento de hechos en los que interviene de alguna forma un recurso electrónico o digital.

La norma proporciona orientación para tratar situaciones frecuentes durante todo el proceso de tratamiento de la evidencia digital. Entre otros fines, pretende ayudar a las organizaciones en sus procedimientos de tratamiento de circunstancias excepcionales, que involucran datos gestionados en ellas de forma que se pueda facilitar el inter-

cambio de evidencias digitales potenciales con los ámbitos jurisdiccionales que sean de aplicación.

Define dos roles especialistas en la gestión de las evidencias electrónicas: experto en primera intervención de evidencias electrónicas (Digital Evidence First Responders o **DEFR**) y el experto en gestión de evidencias electrónicas (Digital Evidence Specialists o **DES**).

La norma **ISO/IEC 27037:2012** proporciona orientación para los siguientes dispositivos y circunstancias:

- Medios de almacenamiento digitales utilizados en ordenadores tales como: discos duros, discos flexibles, discos ópticos y magnetos ópticos, dispositivos de datos con funciones similares.
- Teléfonos móviles, asistentes Digitales Personales (PDA), Dispositivos Electrónicos Personales (PED), tarjetas de memoria.
- Sistemas de navegación móvil.
- Cámaras digitales y de video (incluyendo CCTV).
- Ordenadores de uso generalizado conectados a redes.
- Redes basadas en protocolos TCP / IP y otros.
- Dispositivos con funciones similares a las anteriores.

Entre sus características cabe mencionar:

- Proporciona orientación sobre el manejo de la evidencia digital. Siguiendo las directrices de esta norma se asegura que la evidencia digital potencial se recoge de manera válida a efectos legales para facilitar su aportación a entornos jurisdiccionales (juicios y arbitrajes).
- Cubre toda una gama de tipos de dispositivos y situaciones, por lo que la orientación dentro de la norma es ampliamente aplicable.

2. MODELO DE INVESTIGACIÓN FORENSE

Al indagar en organismos especializados como las Unidades de Delitos Informáticos de la Policía Nacional y de la Fiscalía General de la Nación, organismos que dentro de sus funciones están la de realizar procesos investigativos cuando se presentan delitos que ponen en peligro los principios generales de la información (confidencialidad, disponibilidad e integridad), en entrevistas realizadas a algunos funcionarios de dichas dependencias, se pudo establecer que, aunque sí se están realizando investigaciones por lo menos en niveles básicos y medianamente complejos, su labor se enfoca más a la prevención de dichos delitos que a la persecución de "ciber criminales", hecho que se debe al escaso personal capacitado en técnicas periciales en este campo de la tecnología, junto a la ausencia de herramientas especializadas para la valoración de evidencias. A niveles más complejos, las investigaciones son centralizadas ante la Dirección General de Investigación Criminal e Interpol (DIGIN), pues dicho organismo estatal cuenta con equipos sofisticados y personal altamente entrenado para realizar investigaciones en este campo, hecho que lógicamente hace que en las demás regiones del país, se realicen investigaciones básicas relacionadas, especialmente, con delitos como el hurto bancario a través de dispositivos electrónicos y "delitos menores" contra la información personal, en cuanto al peritaje informático y la labor forense propiamente dicha. Estos cuerpos investigativos se orientan a la recolección y preservación de evidencias, para ser enviadas a la sede central, donde son valoradas y puestas a disposición de la autoridad competente, si el caso así lo amerita.

Paralelamente, se realizó una investigación en universidades de la ciudad de Tunja, con el principio de identificar si existen programas impartidos por ellas que se enfoquen en este campo específico de la informática, al respecto se pudo establecer que a pesar de que existen dos universidades en la ciu-

dad en las que se está capacitando a profesionales en seguridad de la información, éstas ofrecen un enfoque orientado a técnicas de prevención de ataques a sistemas computacionales y dispositivos, donde se entrena en técnicas de cómo pueden ser vulnerados los sistemas informáticos y los dispositivos, pero en lo que tiene que ver con el seguimiento y localización de intrusos, el tema aún se encuentra en una etapa de maduración; en consecuencia, se podría manifestar que el trabajo que hay por hacer en este campo plantea una serie de retos interesantes, que abre nuevos espacios en la comunidad educativa del departamento y de la nación, a su vez que vislumbra un panorama laboral muy atrayente, para quienes opten por profundizar en este tema, ya que es allí donde se debería dar inicio a capacitaciones orientadas a los profesionales y especialistas relacionados con el manejo de información digital. Programas como los que se proponen, muy seguramente evitarán en corto tiempo, que el trabajo que se adelante sobre delitos informáticos se base sólo en experiencias personales y ejemplos teóricos, pasando a hechos de la vida real, donde estos profesionales entren en contacto con técnicas de obtención y validación de pruebas, poniendo su conocimiento y profesionalismo al servicio de las autoridades competentes para la investigación, validación y juzgamiento de conductas atípicas en el campo computacional y de las telecomunicaciones.

Pasando al campo teórico propiamente dicho, es importante resaltar las buenas prácticas que debieran seguirse ante la ocurrencia de un incidente de seguridad, así, los siguientes pasos se hacen muy relevantes para ser tenidos en cuenta si hay que enfrentarse a un posible delito contra la información digital o ante un intento de intrusión o sabotaje informático.

Como es de observarse en la figura 1, la secuencia de procedimientos debe ser realizada por expertos en el tema a fin de su correcta realización; cabe anotar que dichos pasos aunque parezcan redundantes, han sido preparados y concertados por profesionales en el tema y se deben realizar en su totalidad; como parte adicional es importante que, una vez identificadas las pruebas válidas, deben ser destruidas aquellas que no sean útiles y tener compromiso de cooperar con las autoridades judiciales en determinado momento dentro de los casos investigativos que lo ameriten.

Al adentrarse en estudios de la informática forense, se encontró que el profesional indiscutiblemente llegará a plantearse nuevos retos, como conocer acerca de técnicas seguras y válidas de encriptación, uso de herramientas de hardware y software, especialmente diseñados para esta profesión, preparación de informes, técnicas de extracción de pruebas, técnicas de búsqueda en el registro de los sistemas, tablas de asignación de archivos, tablas de partición de discos duros, estructura de los dispositivos de almacenamiento, copias bit a bit, clonación de discos duros, algoritmos hash, sistemas RAID de almacenamiento, diferentes tipos de dispositivos de almacenamiento y transporte de datos, estructura de redes LAN y WAN, métodos de digitalización de información, creación y conservación de una cadena de custodia y muchos otros procesos inmersos en la actividad computacional, dado que gracias al conocimiento de tal temática, muy seguramente se podrá adelantar este tipo de procesos de una forma efectiva y acorde con las necesidades específicas de cada caso en particular, lo que resalta aún más, la experticia con la que debe contar un profesional en investigación de informática forense.

Figura 1. Modelo de Investigación forense.

Fuente: los autores, 2013

Al disponer de los anteriores conocimientos que conducen a afirmar que la Informática forense permite la solución de conflictos tecnológicos relacionados con seguridad informática y protección de datos. Gracias a ella, las empresas y las personas obtienen respuesta a problemas de privacidad, competencia desleal, fraude, robo de información confidencial y/o espionaje industrial, surgidos a través de uso indebido de las tecnologías de la información. Mediante procedimientos muy puntuales se procede a identificar, asegurar, extraer, analizar y presentar pruebas generadas y guardadas electrónicamente para que puedan ser aceptadas en un proceso legal.

De otra parte, se hace indispensable también para el perito informático forense, conocer la normatividad colombiana que regula las actividades relacionadas con la información personal, los sistemas computacionales y las telecomunicaciones, dado que el experto no sólo debe conocer los temas técnicos que rodean la actividad propiamente dicha, sino que además está en la obligación de respetar y hacer respetar la normatividad que protege los datos personales de cada ciudadano en particular. En tal virtud es conveniente tener en cuenta las siguientes normas:

- **Ley 1273 de 2009** "Hace referencia a los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos".
- **Art. 269 del Código Penal Colombiano** "de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" [3].
- **Proyecto de Ley 241 de 2011** "Por la cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en Internet."
- **LEY 1581 de 2012 Decreto 1377** "La cual fue creada con la finalidad de proteger los datos personales" [8].

3. RESULTADOS

Con la exploración de campo y las respectivas indagaciones, se pudo conocer de primera mano diferentes técnicas y procedimientos para la recopilación de evidencia digital, temas base para iniciar un estado del arte a nivel regional en lo relacionado con este tema específico que motivó el presente artículo, se puede deducir que aunque existen personas trabajando fuertemente para estar acorde con las exigencias que esta actividad demanda, la realidad es que aún se requiere de una capacitación completa, funcional y un buen nivel de conciencia para el manejo de la información, así como la formulación, implementación y seguimiento de políticas de seguridad para las empresas, realidades que dejan muchas expectativas y preocupaciones en virtud de la poca atención prestada a este tema de seguridad con la infor-

mación; sin el buen uso de métodos seguros para el adecuado manejo de datos confidenciales, que no solo involucra un riesgo para el funcionario a cargo de dicho activo, sino también la peligrosa exposición a las que de forma natural dejan su información personal en manos de terceros por requerimientos momentáneos, sin preocuparse por un instante en lo que pueda pasar con ellos o para qué propósitos estos datos pueden ser empleados.

Otro aspecto altamente preocupante que se encontró, es el escaso personal capacitado para realizar procesos seguros para el manejo de la información y la realización de un adecuado peritaje, dado que un evento contra la seguridad de la información digital se anuncia sin preguntar. Estos hechos crean una gran expectativa y dejan un informe concluyente que puede servir de base para la toma de decisiones tendientes a la capacitación de más personal y la adquisición de equipos adecuados a las demandas actuales que permitan reducir e investigar adecuadamente cada caso que se presente, dejando entrever que la aplicación de las herramientas correctas, ayudan a solucionar incidentes de seguridad como los que se describen en el presente artículo. Todos estos aspectos traen como consecuencia lógica, que adelantar un proceso investigativo en este campo sea bastante costoso y poco eficiente, debido a los tiempos que se toma el simple hecho de contactar un experto en el tema, que esté en la capacidad de emitir un informe realmente útil y oportuno para la solución de un caso investigativo tendiente a la persecución y judicialización de un delincuente informático.

Lo que se observa principalmente es la necesidad de recurrir a los organismos oficiales e iniciar largos procesos, que en determinados momentos podrían no obtener óptimos resultados que puedan dar soporte y/o vía a una acción judicial si el caso así lo requiere. Citando una situación de la vida real, ya sea el caso que por un acto voluntario o involuntario se presente un daño en dispositivos de almacenamiento tales como discos duros internos o externos, en el mercado se encuentran aplicaciones que permiten la recuperación de información cuando se presenta un daño lógico (formateo, pérdida de una partición, eliminación o modificación de archivos), pero para el caso de daño físico (daño de cabezales, golpes, daño de platos o motor del disco), por lo menos en lo que se trata localmente en la ciudad de Tunja, no existe una empresa o personal de soporte que realmente esté capacitado y sea reconocido, además de estar certificado para realizar tales procedimientos de recuperación, hecho que trae como consecuencia directa que se deba recurrir a empresas de índole nacional o transnacional lo que representa costos muy elevados y demorados ante un evento de seguridad como éste.

Si bien es cierto, estas unidades son dispositivos realmente sensibles a daño o golpes, la tecnología actual está trabajando en el diseño de nuevas formas de almacenamiento en la nube (Clouding) o fabricación de otro tipo de discos como los Discos de estado sólido o SSD (Solid-State Drive) [4], que son dispositivos de almacenamiento de datos que usan una memoria no volátil, como la memoria flash, o una memoria volátil como la SDRAM, para almacenar datos, en lugar de los platos giratorios magnéticos encontrados en los discos duros convencionales. En comparación con los discos duros tradicionales, las unidades de estado sólido son menos sensibles a los golpes, son prácticamente inaudibles y tienen un menor tiempo de acceso y de latencia. Las SSD hacen uso de la misma interfaz que los discos duros y, por lo tanto, son fácilmente intercambiables sin tener que recurrir a adaptadores o tarjetas de expansión para compatibilizarlos con el equipo. Se han desarrollado también dispositivos que combinan ambas tecnologías, es decir, discos duros y memorias flash, y se denominan discos duros híbridos (HHD), que intentan aunar capacidad y velocidad a un precio inferior a un SSD.

Aunque esto promete dar una solución para este problema específico (golpes o daños físicos), por otra parte, se deberá continuar luchando por tener profesionales aptos para la recuperación de infor-

mación por daño lógico o físico, y que estén en la disponibilidad de rastrear y recuperar información en dispositivos locales o de red, proceso que forma parte de la tarea del investigador forense o profesional en el manejo de la información digital.

Las aplicaciones de software y las herramientas de hardware descritas en la tabla 1, brindan la posibilidad de conocer su existencia y sobre el manejo de muchas de estas herramientas, las cuales poseen una gran cantidad de aplicativos especializados que pueden ser útiles en eventos muy puntuales como el rastreo de direcciones IP, descifrar claves de diferentes archivos o dispositivos, programas para crear copias fieles de sistemas completos de archivos, realización de algoritmos hash que garantizan la inalterabilidad de una cadena de custodia, recuperación de todo tipo de datos en distintos dispositivos de almacenamiento y en sistemas de archivos diferentes (NTFS, FAT, SWAP, Ext, entre otros). Procesos que ponen en evidencia que, sabiendo utilizar estas herramientas tecnológicas adecuadamente, la labor del investigador forense digital, muy seguramente será relevante a la hora de resolver casos o investigaciones puntuales.

Ahora el tema esencial es el de profundizar en lo relacionado con las formas de hacer legalmente válidas estas pruebas recolectadas, lo que plantea un nuevo reto para el profesional experto en este campo de la computación y el cual consiste en capacitarse también en procedimientos judiciales, tendientes a no invalidar una prueba, pues está completamente demostrado que un mal procedimiento puede echar abajo un proceso investigativo y penal, si no se tienen las respectivas precauciones para su obtención, cadena de custodia y presentación ante un estrado judicial cuando el caso así lo requiera. Casos muy sonados como el de los computadores del exjefe guerrillero Raúl Reyes, hallados en el sitio donde fue abatido por los organismos del estado, muestran cómo aunque esa evidencia sea realmente probatoria y contengan una verdad irrefutable, un mal procedimiento o una falla dentro de la cadena de custodia, deja sin validez esas pruebas y evidencias digitales que a la postre, quedaron almacenadas y por lo menos hasta ahora, pasaron a ser información con poca relevancia para los organismos encargados de validar y certificar que se trata de información realmente valiosa para ser usada en un proceso judicial.

Tabla 1. Herramientas informáticas para el análisis forense

Herramienta	Características
X-ways forensics	El software **X- WAYS** [5] Contiene un Kit de herramientas compatibles con versiones de Windows 2000/XP/Vista/Seven/ 2008 y tecnologías de 32 y 64 bits. Posibilita crear imágenes o copiados seguros de evidencias digitales, recuperación de información eliminada, visualización de estructuras de directorios sobre imágenes del tipo .dd. Acceder a discos, RAIDs, e imágenes de gran tamaño (2Tb), creación de medios forenses estériles, entre otros.
Amped five professional forensic	El software **AMPED FIVE PROFESSIONAL FORENSIC** [6] presenta un kit de herramientas forenses para la recuperación y análisis de fotos y videos. Registra cada paso dado en la mejora del archivo y genera un informe, que puede ser incorporado en los requisitos de información de la Agencia.

Herramienta	Características
Deft Linux computer forensic	**DEFT LINUX COMPUTER FORENSIC** (Digital Evidence & Forensic Toolkit - DEFT) [6] es una distribución Live CD (booteable desde el CD), basada en Linux Ubuntu con un amplio listado de herramientas forenses y con una excelente detección del hardware, está dividida en dos interfaces, su entorno y herramientas booteables permiten el análisis forense y DEFT Extra un conjunto de herramientas gratuitas para análisis forense en entornos Windows.
Elcom password recovery 2013	**ELCOM PASSWORD RECOVERY 2013** [6] es útil para recuperar cualquier tipo de clave que se haya olvidado; no importa si es de Word, Excel, WinZip o de un usuario de nuestro sistema, cuenta con una herramienta especializada para cada problema.
Ilook investigator forensic	El software **ILOOK INVESTIGATOR FORENSIC** [6], es un completo conjunto de herramientas forenses informáticas. ILOOK Investigador incluye: ILOOK aplicación forense v8 y el IX imager; ambos están diseñados para seguir las mejores prácticas forenses. Puede ser utilizado para examinar imágenes obtenidas de cualquier sistema de formación de imágenes forenses que crea un volcado del sector consecutivo de los medios de comunicación con imagen. También puede ser utilizado para examinar los archivos de imagen SafeBack, En Case archivos de imagen ISO y CIF imágenes de los CD, discos virtuales VMWare y archivos de imagen ILOOK.
Máquina especializada para cambio de integrados de las tarjetas lógicas de los discos duros. **Sistema raid de 1,0,5,10,50**	El procedimiento que se hace en la recuperación de información [7]: En el caso de servidores, hay que verificar la tecnología del Disco, si es Sata, SCSI o SAS y en el caso de los RAID, hay que verificar si son RAID O, RAID 1 O RAID 5 para evaluar la posibilidad de la recuperación de la información y si es necesario reparar el disco o no, o los procesos necesarios para recuperar la información. Si desea tener más claro el funcionamiento de las diferentes configuraciones RAID.
Recuperación de platos de un disco duro en ambiente estéril.	Este procedimiento permite la recuperación de datos en dispositivos de almacenamiento fijo (disco duros Sata o IDE) usados en PC personales ya sean de escritorio o portátiles [7]. Estos discos se componen de platos de metal donde se guarda la información con base en las estructuras de cada fabricante. También se componen de tarjetas lógicas y otros elementos electrónicos para su funcionamiento. Las recuperaciones varían de acuerdo con la complejidad de cada caso.
Cambio de cabezales de lectura de un disco duro rígido	La empresa de recuperación realiza este procedimiento [7] **con un clean room** (Sala Limpia), en la cual se realizan los procesos de cambios de cabezales y platos cuando se requiere. Los discos duros no están al vacío, solamente libres de partículas. Una sola partícula o "mota", si entra en contacto con los platos de los discos duros, puede dañar de manera definitiva la información.

Fuente: los autores, 2013

4. DISCUSIÓN

En este tema vale la pena hacer la pregunta ¿realmente estamos preparados para proteger nuestra información y conocemos la norma para hacer valer ese derecho fundamental de respetar nuestra privacidad reposada en dichos datos?

Aunque la Ley 1273 de 2009 regula claramente y expone una serie de penas cuando se presentan atentados contra los principios básicos de la información, como lo son, la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. La verdad es que como la mayoría de leyes en Colombia, aunque están fundamentadas, su aplicabilidad deja mucho que desear, especialmente si carece de profesionales expertos que ayuden, orienten y sepan cómo obtener legalmente pruebas que nos ayuden a hacer valer nuestro derecho constitucional, al buen uso de la información personal que es depositada en manos de terceros y el cómo rastrear, ubicar y ayudar a capturar individuos que violen esos principios fundamentales y pretendan o usen tal información para atentar contra otros derechos como el prestigio, la honra e incluso hasta nuestra propia vida.

Otra norma en la que se basa este principio es en la Ley Estatutaria 1581 de octubre 17 de 2012 [8], que en su artículo 1° Objeto**,** dispone lo siguiente**: "**La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política en sus Principios Fundamentales (Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas); así como el derecho a la información consagrado en el artículo 20 de la misma".

Entonces, basados en los anteriores preceptos, se debe hacer un examen riguroso tendiente a identificar si la ciudadanía en general está realmente informada al respecto, si las instituciones de índole nacional y/o local han emprendido o dentro de sus planes tienen dispuesto, enfrentar esta problemática con eficacia y contundencia o si solo se trata de una ley muerta que se conoce exclusivamente cuando se presenta un fraude de estas magnitudes y el ciudadano se ve enfrentado a la necesidad de conocer y exigir el cumplimiento de la norma que regula los aspectos numerados anteriormente.

Ahora la pregunta sería, ¿cuál es el verdadero papel de nosotros como profesionales especialistas en seguridad de la información, conocedores de la norma y de métodos seguros para la protección y disposición de este valioso activo? ¿Hasta dónde va nuestra obligación de velar por los principios también descritos en el presenta artículo y cómo debemos hacer frente de una manera adecuada a esta problemática?

Muy seguramente las respuestas a las anteriores preguntas terminarán por resaltar el papel fundamental que, a partir de ahora, profesionales en áreas como **Seguridad de la Información** deben cumplir, partiendo desde el entorno familiar, personal y hasta el laboral, para llegar a crear y liderar procesos de capacitación, concientización en el manejo seguro de nuestra información, procesos adelantados con las empresas, con personas naturales para las cuales se cumplirá la labor en defensa de los datos, que sin lugar a dudas se han convertido en el bien más preciado para las instituciones públicas y privadas.

5. CONCLUSIONES

Como conclusión general se puede indicar que, por lo menos en este campo, hay una excelente oportunidad de formación profesional y de negocio para quienes estén con la convicción de capa-

citarse a profundidad; enfocando sus esfuerzos a convertirse en consultores de seguridad, investigadores forenses, expertos en el manejo y recuperación de la información, en docentes competentes que sean multiplicadores de soluciones y de formas de minimización de esta problemática, o desenvolverse en una gran cantidad de actividades relacionadas con esta materia, tal como lo podría llevar a cabo un profesional en peritaje informático.

De otro lado, la falta de conocimientos específicos en el área informática forense por parte de los profesionales en Derecho, requiere de profesionales en sistemas y en seguridad de la información, para que a la hora de presentar pruebas dentro de un proceso penal, se cuente con el concepto de un experto en este campo, el cual pueda cumplir las veces de perito y a su vez sirva como testigo clave en un proceso llevado a cabo, como consecuencia de un delito cometido contra la información digital y los dispositivos que la contienen y permiten su respectivo procesamiento.

Al adentrarse en este tema, es posible manifestar que en nuestro diario vivir, específicamente en el tema de seguridad de la información se puede verificar que existen empresas estatales y particulares que aunque cuentan con políticas de seguridad plasmadas documentalmente y que son la base para evitar delitos informáticos, en la realidad no están llevadas a cabo cada una de estas prácticas que en su inicio fueron determinadas para el buen uso y desempeño de las funciones a la hora de salvaguardar información. Normalmente se crean más con el fin de cumplir un requisito frente a la finalidad para la cual fue creada la organización, que resaltar la verdadera importancia que tiene la información dentro de cada uno de los procesos que desarrollan las compañías.

Otro hecho que deja la indagación realizada en la investigación de campo, es la forma como se está llevando a cabo el proceso formativo, donde se enfoca más a enseñar cómo vulnerar sistemas computacionales (hecho que indudablemente importa para saber cómo llegan los delincuentes a penetrar sistemas), pero después de ese tipo de capacitación, se debiera fortalecer aún con mayor intensidad las técnicas de seguimiento, rastreo y ubicación de delincuentes, que finalmente es lo que más importa a la hora de ejercer éticamente la labor forense.

Así como los sistemas avanzan a pasos agigantados, se hace necesario que las demás disciplinas vayan a un mismo nivel de desarrollo para evitar inconsistencias a la hora de tomar determinaciones que por falta de herramientas acordes, normatividad y/o estándares, se deje de lado cualquier interpretación.

Se hace necesario, fortalecer procesos de formación específica en el campo de la computación forense, que ayuden a establecer los protocolos válidos en técnicas de recolección de evidencia digital.

Ahora bien, si actualmente eres un profesional orientado al estudio de una especialización en seguridad de la información, puedes enfocar parte de tus estudios a la profundización de las cinco palabras clave que, como autores del presente artículo, dejamos a disposición. Es ideal que no solamente queden aquí plasmadas sino que junto a nosotros conformen un grupo pionero de retos ante estas disciplinas y dar un valor agregado a nuestra profesión.

AGRADECIMIENTOS

A la Fundación Universitaria Juan de Castellanos, al programa de Especialización en Seguridad de la Información de la Facultad de Ingeniería, que a través del grupo profesional docente nos orientaron la especialización en Seguridad de la Información, las Instituciones encargadas en procedimientos de delitos informáticos a nivel regional, a profesionales y personas involucradas en el tema, quienes nos aportaron en nuestro crecimiento profesional, el cual plasmamos en el presente artículo.

REFERENCIAS

[1] J. Inze, (2013), Directrices de gestión de evidencias electrónicas, Todo es Eletrónico. Noticeman EAD Trust, ISO 27037, [On line]. Disponible en http://inza.wordpress.com/2013/06/11/ iso-27037-directrices-de-gestion-de-evidencias-electronicas/

[2] Congreso de la República, (2013), Diario Oficial No. 47.223 del 5 de enero de 2009 - LEY 1273 DE 2009 - CAPÍTULO I - De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, [On line]. Disponible en http://www.secretaria senado.gov.co/senado/basedoc/ley_ 1273_2009.html

[3] Congreso de la República, (2013, diciembre), Código Penal, De la protección de la información y de los datos, Senado de la República de Colombia, Información legislativa, [On line]. Disponible en http://www.secretaria senado.gov.co/senado/basedoc/ley/2000/ley_0599_2000_pr010.html

[4] Enciclopedia Electrónica Wikipedia, Unidad de Estado Sólido, [On line]. Disponible en http://es.wikipedia.org/ wiki/ Unidad_de_estado_s%C3%B3lido

[5] Forensics Project, (2012) Herramienta X-Ways Forensics usada en la informática forense, [On line]. Disponible en http://www.forensics-project.org/2012/03/x-ways-forensics-avanzado-entorno-de.html

[6] Laboratorio Forense, (2013), Herramientas en la informática forense, [On line]. Disponible en https://sites.google.com/site/sykrayolab /informatica-forense

[7] SOS Datos, (2013). Recuperación de Datos, [On line]. Disponible en http://www.sosdatos.com/

[8] Congreso de Colombia, (2012, octubre), Diario Oficial, Ley Estatutaria 1581 de 2012, Disposiciones generales para la protección de datos personales, [On line]. Disponible en http://www.alcaldiabogota.

gov.co/sisjur/normas/Norma1.jsp?i=49981

[9] Digital Recovery, (2013, diciembre), Recuperación de datos, [On line]. Disponible en http://www.digitalrecove ry.com.co/informatica-forense-colombia. htm

[10] M. Gallardo, (2013), Perito Informático Forense, [On line]. Disponible en http://www.miguelgallardo.es/perito /informatico/

[11] Master Recovery Labs, (2013), Recuperación de datos y peritaje forense, [On line]. Disponible en http://www. masterrecoverylab.co/ servicios.asp

[12] Periódico El Universal, (2013, septiembre), Así funciona la informática forense en Colombia, Sección Tecnología, Cartagena, Colombia, [On line]. Disponible en http://www.eluniversal.com.co/tecnolo gia/asi-funciona-la-informatica-forense-en-colombia-134018.

[13] Periódico El Universal, (2013, octubre), Medio millón de personas son víctimas de hackers, – Sección Tecnología, Cartagena, Colombia, [On line]. Disponible en http://www.eluniversal. com.co/tecnologia/medio-millon-de-personas-diariamente-son-victimas-de-hackers-139247

[14] Policía Nacional de Colombia, Unidad de Delitos Informáticos, Recomendaciones de Seguridad, [On line]. Disponible en http://www.policia.gov.co/portal/page/portal/UNIDADES_POLICIALES/Direcciones_tipo_Operativas/Direccion_Seguridad_Ciudadana/Planes_de_Seguridad/Recomendaciones_de_seguridad/delitos_informaticos

[15] Mattica, Seguridad de la Información y la Informática forense. [On line]. Disponible en http://www.mattica.com/

[16] Certicamara, (2013, agosto), Colombia Digital, ABC para proteger los datos persona-

les, Ley 1581 de 2012 Decreto [On line]. Disponible en http://www. colombiadigital.net/entorno-digital/ articulos-de-contexto/item/5543-abc-para-proteger-los-datos-personales-ley-1581-de-2012-decreto-1377-de-2013.html

[17] A. Montoya, La Informática Forense como Herramienta para la Aplicación de la Prueba Electrónica, Estudios Jurídicos de la Universidad CES. [On line]. Disponible en http://www.google. com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CDcQFjAC&url=http%3A%2F%2Frevistas.ces.edu.co%2Findex.php%2Fderecho%2Farticle%2Fdownload%2F1289%2F807&ei=AIfaUsy6EYWvkAehr4DoBQ&usg=AFQjCNH1Pm4XUXLA5FhG3qHM3kfl26YbbQ

[18] J. R. Vacca, Computer Forensics, Computer Crime Scene Investigation, Second Edition, 2013.

[19] C. Easttom, J. Taylor, Computer Crime, Investigation and the Law, Course Technology, 2011.

[20] A. Marcella, R. Greenfield, Cyber Forensics, CRC Press, 2002.

[21] EC-Council, (2013), Modulo de Computer Hacking Forensic Investigator (CHFI), [On line]. Disponible en http://www.eccouncil.org/Certification/ computer-hacking-forensics-investigator

[22] Clarke Nathan, Computer Forensics, A Pocket Guide, 2010.

[23] B. Nelson, et al., Guide to Computer Forensics and Investigations, 3rd. edition, Cengage, BBS, 2010.

[24] T.J. O´Connor, Violent Python, A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers, Syngress, 2012.