# FORENSIC ANALYSIS IN INFORMATION SYSTEM IN THE COLOMBIAN LEGAL FRAMEWORK

# ANÁLISIS FORENSE EN UN SISTEMA DE INFORMACIÓN EN EL MARCO NORMATIVO COLOMBIANO

**Recibido: 28 de junio 20 14 - aceptado: 18 de octubre 2014**

**Cesar Villamizar.**[1]
**Universidad de Pamplona**

**Ailin Orjuela.**[2]
**Universidad de Pamplona**

**Marco Adarme.**[3]
**Universidad Francisco de Paula Santander**

**Keywords:**
Forensics analysis, computer crime, information system, regulations.

**Abstract**
Forensic analysis is to determine the causes of compromise security of a system. At present general rules and principles as the International Organization for Digital Evidence (IOCE) they are known. The aim of the study was to characterize Colombian law as to the specific and necessary for the design of computer technical regulations regarding the extraction of digital evidence to anchor the chain of custody. A descriptive documentary research and applied type was used, by analyzing different sources on information systems, integrity, confidentiality and availability of data in judicial custody. Current regulations allow substantiate the use of computer techniques to extract digital evidence and ensure the chain of custody, based on the constitutional protection of the right to privacy, so they must respect freedom and promote other warranties. Regulations also relies on Law 527 of August 18, 1999 which is magnetic and software tools, as well as the law 527 of 1999 on electronic commerce for Colombia, Law 1273 of 2009 for the protection of information and Law 1273 of 2009 which criminalizes cybercrime.

**Palabras clave:**
Análisis forense, delito informático, sistema de información, normatividad.

**Resumen**
El análisis forense consiste en determinar las causas del compromiso de seguridad de un sistema. En la actualidad se conocen normas y principios generales como la Organización Internacional en Evidencia Digital (IOCE). El objetivo del estudio fue caracterizar la legislación colombiana en cuanto a la normatividad específica y necesaria para el diseño de la técnica informática en cuanto a la extracción de la evidencia digital para anclar la cadena de custodia. Se utilizó una investigación descriptiva de tipo documental y aplicada, mediante el análisis de diferentes fuentes sobre sistemas de información, integridad, confidencialidad y disponibilidad de datos bajo custodia judicial. La normatividad actual permite fundamentar el uso de técnicas informáticas para la extracción de la evidencia digital y asegurar la cadena de custodia, basado en la protección constitucional del derecho a la intimidad, por lo que se deben respetar la libertad y promover las demás garantías. También la normatividad se apoya en la Ley 527 de Agosto 18 de 1999 que trata de los instrumentos magnéticos e informáticos, así como la ley 527 de 1999 sobre el comercio electrónico para Colombia, la Ley 1273 de 2009 para la protección de la información y la Ley 1273 del 2009 que tipifica los delitos informáticos.

1. Universidad de Pamplona. Norte de Santander, Colombia.
2. Universidad de Pamplona. Norte de Santander, Colombia.
3. Universidad Francisco de Paula Santander. Norte de Santander, Colombia.

*Este artículo es asociado al proyecto de investigación : Análisis Forense En Un Sistema De Información En El Marco Normativo Colombiano

## I. INTRODUCCIÓN

El análisis forense en sistemas de información permite obtener evidencias concretas de los diferentes dispositivos o elementos que no se deben alterar durante el proceso investigativo. [1] Por ésta razón es fundamental recopilar la evidencia digital y anclarla a la cadena de custodia, por lo cual los laboratorios forenses necesitan de herramientas eficaces que acompañen la preparación, el conocimiento y las técnicas de toma de evidencia que sirvan como elemento probatorio en los procesos judiciales encargados de atender este tipo de delitos informáticos.

Al analizar las enunciaciones por parte de los organismos judiciales en cuanto a las personas y delitos que se comenten en el área informática, se encuentra a la Organización Internacional de Policía Criminal [2] quien afirma que la ciberdelincuencia constituye uno de los ámbitos delictivos de más rápido crecimiento. Cada vez más delincuentes se aprovechan de la rapidez, la comodidad y el anonimato que ofrecen las tecnologías modernas para llevar a cabo diversos tipos de actividades delictivas.

Este tipo de delitos incluyen ataques contra sistemas y datos informáticos, usurpación de la identidad, distribución de imágenes de agresiones sexuales contra menores, estafas, subastas realizadas a través de Internet, intrusión en servicios financieros en línea, difusión de virus, botnets (redes de ordenadores infectados controlados por usuarios remotos) y distintos daños por correo electrónico, como el phishing (adquisición fraudulenta de información personal confidencial) para acceder a la información de los servidores sin control. [3]

Actualmente, no existe una técnica apropiada para la recolección de evidencia digital en nuestra legislación, ni protocolos, al punto que el manejo de los sistemas de información permitan extraer la prueba digital, para anclar la cadena de custodia, no cuentan con una técnica sistemática que ayude a mantener integra, segura, idónea y original la evidencia digital, como lo exige el ordenamiento procesal colombiano, según la ley 597 del 1999.

Conforme a lo anterior, el presente estudio tiene como propósito caracterizar la legislación colombiana en cuanto a la normatividad específica y necesaria para el diseño de la técnica informática en cuanto a la extracción de la evidencia digital para anclar la cadena de custodia. [4]

## II. METODOLOGÍA

El nivel de investigación fue descriptivo, fundamentado en Palella y Martins [5] ya que “permite el registro, análisis e interpretación de la naturaleza actual de un hecho o fenómeno”. Por otra parte Arias 2006 dice, “El nivel de la investigación se refiere al grado de profundidad con que se aborda un fenómeno u objeto de estudio” [6].

El diseño de la investigación es de tipo documental, de acuerdo con Arias [6] teniendo en cuenta que “la investigación documental es un proceso basado en la búsqueda, recuperación, análisis, critica e interpretación de datos secundarios, es decir, los obtenidos y registrados por otros investigadores en fuentes documentales”. (p.27).
También Palella y Martins [5] definen la investigación documental “como la recopilación de información en diversas fuentes. Indaga sobre un teme en documentos escritos u orales”.

Según el objeto de estudio desarrollado, el proyecto se enmarcó en un enfoque de investigación aplicada, con la finalidad de resolver problemas técnicos que permitan controlar situaciones prácticas. [7]
Las fuentes de información fueron secundarias basadas en documentos, libros y textos sobre sistemas de información, integridad, confidencialidad y disponibilidad de datos bajo custodia judicial. También se tuvieron en cuenta las demás fuentes bibliográficas y electrónicas relacionadas con el tema.

Las principales fuentes de información para el desarrollo de la investigación fueron documentos de la Unidad de Delitos Informáticos del Cuerpo Técnico de Investigaciones de la Fiscalía General de la Nación de Santander, cuyas estadísticas tienen la condición de documento reservado. [8]
Documentos de la Unidad de Delitos Informáticos de la DIJIN – Policía Nacional, cuyas estadísticas tienen la condición de documento reservado.
Apuntes de derecho informático de Alexander Díaz García - Juez de la Republica autor de la Ley 1273 de delitos informáticos en Colombia. [9].

Computación Forense, Descubriendo Los Rastros Informáticos de Jeimy Cano.
Delitos informáticos en el ciberespacio de Luis Orlando Paloma Parra. [10]
Hackers aprende a atacar y a defenderse de Julio Gómez López.

La información obtenida se procesó por medio de técnicas descriptivas para comprender y sinterizar mejor los resultados, por medio de tablas estadísticas y graficas de barras, que fueron procesados por medio de una hoja de cálculo.

## III. RESULTADOS

### *A. Los sistemas de información y delitos informáticos.*

En la actualidad se observa el acelerado desarrollo de los avances tecnológicos y de los sistemas de información; este desarrollo ha generado efectos positivos para el crecimiento económico, social, cultural de las naciones. Según cifras registradas por el Departamento Administrativo Nacional de Estadística DANE [11] reportó un crecimiento en la utilización de los sistemas de información en el país, observándose que en el total nacional, el 38,4% de los hogares poseía computador de escritorio o portátil; 46,8% en las cabeceras y 8,4% en resto.

Figura 1. Histórico de delitos informáticos

Estas cifras reportadas, evidencian el acceso a los sistemas de información y la importancia que estos mecanismos, imprimen al desarrollo social, cultural y económico; no obstante también ha ocasionado el aumento de sucesos criminales, que en un alto porcentaje dejan tras de sí evidencias digitales en los dispositivos de almacenamiento o en la red. [12]

Estos delitos o sucesos criminales lo contextualizan los expertos como delitos clásicos realizados desde los sistemas de información y delitos informáticos; según Díaz Alexander [13] "El delito informático es la conducta que vulnera la información y el dato privado, mientras que el delito clásico informático se entiende como el ilícito consumado a través de medios electrónicos".
Según Estadísticas de la Policía Nacional, los delitos informáticos representados por su ocurrencia, han aumentado en gran porcentaje a través del tiempo, por el mayor acceso de las personas a los sistemas de información, tal como lo muestra las figura 1.

Figura 2. Histórico de delitos informáticos

De la misma forma, de acuerdo al tipo de delito informático según cifras de la Policía Nacional [7] que los incidentes de con dominios gov y edu en cuanto a Defaced, Phishing, Malware, C&C, han venido disminuyendo, debido a la captura y judicialización de los mismos. [14].

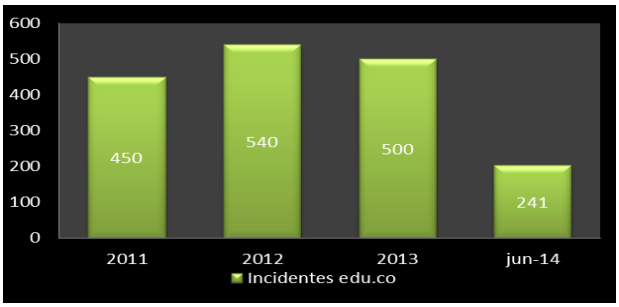

Figura 3. Delitos informáticos, incidentes con dominios edu [15]

Al observar en detalle se encuentra que al 2014, que el delito defaced es el de mayor representación, ocasionando el deterioro de las páginas de web, siendo así las más atacada las páginas que tienen relación con instituciones educativas casi el doble más que las páginas web gubernamentales. [16]

Figura 4. Delitos informáticos, incidentes con dominios gov [15]

En Cúcuta, según como lo muestra la gráfica el hurto por medios informáticos y semejantes es el mayor de los delitos informáticos, observando una disminución en el año 2014 con respecto al 2013 y 2012. [17]

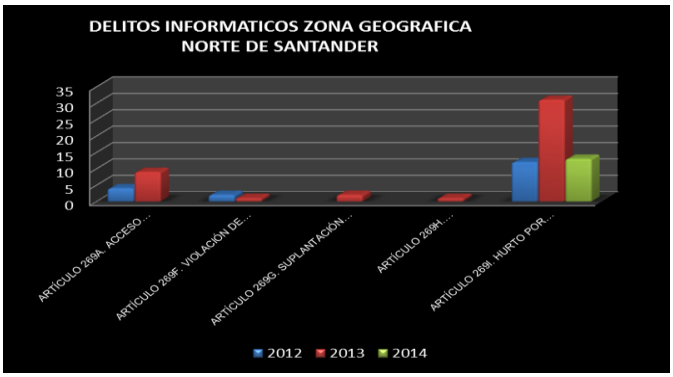


Figura 5. Delitos de sistemas de información por zona geográfica Norte de Santander [15]

En Norte de Santander refleja el mismo comportamiento de Cúcuta, tal como lo muestra la gráficas 17 siguiente, con respecto a los incidentes informáticos el hurto por medios informáticos y semejantes es el de mayor representación. [18]

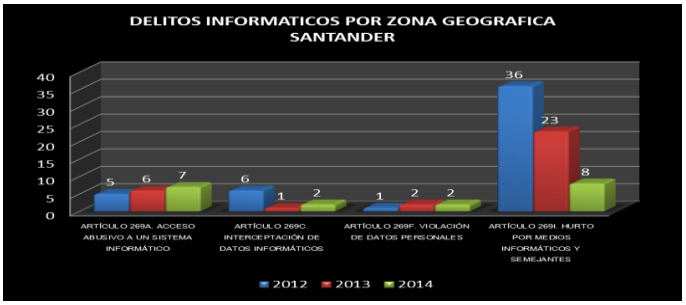


Figura 6. Delitos de sistemas de información por zona geográfica Santander [15]

La zona geográfica de Santander y el incidente informático hurto por medios informáticos y semejantes, según como lo muestra la gráfica 19 es el de mayor representación, cabe resaltar que con una disminución representativa en el año 2014. [19]

*B. Cadena de custodia.*

Cuando se hace referencia a la cadena de custodia el Código Penal Colombiano en su artículo 254 establece como son los procedimientos, en el desarrollo de un proceso judicial y la conservación de las pruebas en las investigaciones, buscando que las mismas no sean alteradas o cambiadas, a lo cual se le da nombre de cadena de custodia.

La cadena de custodia es un procedimiento documentado que es utilizado para comprobar que los elementos materiales que son pruebas en un proceso y su evidencia física cumplan las condiciones de identidad, integridad, preservación, seguridad, almacenamiento, continuidad y registró. [20]

En este sentido el artículo 254 del Código penal dice: "artículo 254. Aplicación. Con el fin de demostrar la autenticidad de los elementos materiales probatorios y evidencia física, la cadena de custodia se aplicará teniendo en cuenta los siguientes factores: identidad, estado original, condiciones de recolección, preservación, embalaje y envío; lugares y fechas de permanencia y los cambios que cada custodio haya realizado. Igualmente se registrará el nombre y la identificación de todas las personas que hayan estado en contacto con esos elementos. [21]

*C. La evidencia digital.*

La evidencia digital comprende la información en forma digital que puede constituir el hecho que relacione un delito con la persona que lo origino; siendo esta primordial como prueba en un proceso judicial. Según HB: 171 Guidelines for the Management of IT Evidence, es ""cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático"; es decir es un concepto utilizado para referirse a cualquier registro creado o almacenado de un sistema informático que constituye prueba en un proceso judicial. [22]

Según Martínez [23] la "Evidencia Digital es un tipo de la evidencia física, que es menos tangible que otro tipo de evidencias, pero a diferencia de todas las demás evidencias físicas, esta presenta ciertas ventajas, debido a que puede ser duplicada de una forma exacta, por lo que es posible peritar sobre copias, tal cual como si se tratara de la evidencia original, lo cual permite realizar diversos tipos de análisis y pruebas sin correr el riesgo de alterar o dañar la evidencia original".

Por lo tanto esta clase de evidencia constituye una fuente útil en la resolución de procesos judiciales, en los cuales la necesidad de información, requiere un análisis detallado que permita al investigador la no alteración de la evidencia digital original y que determine la certeza que no va ser modificada en la manipulación de la misma. [24]

En el mismo sentido, se puede afirmar que la evidencia digital no puede ser destruida fácilmente y es fuente

importante en la hora de resolver un delito, relacionada con esta.

Reconocimiento de la evidencia digital. La informática forense encargada del estudio de la evidencia digital, como prueba en casos judiciales, enfatiza en la importancia de la utilización de la terminología adecuada para el reconocimiento de un delito informático. Cabe señalar, que esto es para enfocar correctamente el proceso, la consecución de indicios y posteriormente la preparación de elementos probatorios necesarios para sostener el caso. Es así como el procedimiento de un proceso por asesinato en donde se halle evidencia digital es diferente al que se maneje para una estafa informática. [25]

Por esta razón, el papel que cumple el sistema informático en estos casos es muy importante, ya que este es, el que fijara como debe ser encontrada y como se debe emplear la evidencia. Para tal fin, la informática forense ha creado cualidades con el propósito de diferenciar el elemento material evidencia electrónica y el contenido en este evidencia digital.

## IV. DISCUSIÓN

El contexto jurídico colombiano, estructura dentro del sistema una normativa amplia sobre la prueba en los procesos judiciales. Esta normativa contiene el desarrollo de las doctrinas y jurisprudencia, con el propósito de establecer el medio probatorio en una herramienta poderosa en la resolución de procesos judiciales. [26]

La constitución política de Colombia en su artículo 15 establece "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. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley" dando origen a lo que sería la ley de habeas data, protección de datos personales e intimidad. [27]

La ley 527 de 1999 ley de comercio electrónico para Colombia, reglamenta y define el uso y acceso del mensaje de datos, comercio electrónico, firmas digitales y empresas certificadoras. [28]

En el artículo 11 de la ley del documento electrónico, dice que para la estimación de la fuerza probatoria de los mensajes de datos ha de considerarse las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas, entonces se debe tener en cuenta: la confiabilidad en la forma que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma como se identifica su iniciador y cualquier otro factor pertinente. [29]

Por otra parte, en el artículo 12 cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho, siempre que se cumplan las siguientes condiciones:

1. Que la información que contengan sea accesible para su posterior consulta.

2. Que el mensaje de datos o el documento sea conservado en el formato en que se haya generado, enviado o recibido o en algún formato que permita demostrar que reproduce con exactitud la información generada, enviada o recibida, y

3. Que se conserve, de haber alguna, toda información que permita determinar el origen, el destino del mensaje, la fecha y la hora en que fue enviado o recibido el mensaje o producido el documento.

Constituyendo así la ley, una garantía de los medios probatorios en los procesos judiciales de registros informáticos. Tal afirmación Díaz [30] dice que "la ley del documento electrónico, nos dice que para la valoración de la fuerza probatoria de los mensajes de datos ha de considerarse las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas, entonces se debe tener en cuenta: la confiabilidad en la forma que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información".

Ley 1273 de 2009 estructura la protección de la información y de los datos y se preservan integralmente, los sistemas que utilicen la tecnología de la información y las comunicaciones, determina cuales son los hechos que determinan vulneración de la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. [31] Enfatizando el acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales y suplantación de sitios web para capturar datos personales. [32]

En este contexto, en Colombia la tecnología e informática es de fácil acceso por la sociedad, siendo expuestos a ser víctimas de ataques informáticos, [33] en esta ley se determinan las acciones por parte del gobierno colombiano y sus entidades contra este flagelo.

La ley 1273 del 2009 tipifica los delitos informáticos con el fin de penalizar a los infractores. [32]

Igualmente en Colombia solo existe legislación en delitos informáticos y manejo de mensajes de datos la ley 527 si bien habla de en su artículo 8 de la originalidad.

La ley habla de originalidad, integridad y autenticidad pero las organizaciones empresariales no saben cómo aplicar estos artículos a través de la informática forense toda evidencia digital tiene que ser sometida a estándares internacionales, entre otros, la extracción de metadatos y/o datos volátiles, si el ordenador esta encendido y la impresión de la huella hash para anclar a continuación la cadena de custodia. [34]

El hecho de haber abierto un documento pero sin manipular la información, [35] no existe certeza para el Juez de Conocimiento ora el Juez de Control de Garantías, sobre la autenticidad del mismo, porque la integridad de él se ha puesto en duda.

Abrir un documento electrónico y simplemente recorrer el cursor dentro del mismo sin estampar ningún carácter alfa numérico, no quiere decir exactamente que no haya sido alterado, así no se observe ninguna información aparente, porque efectivamente si se alteró la cantidad de caracteres, al ser un número mayor al original, cuando el autor lo almacenó por última vez o para cuando lo creó la primera vez. Actualmente los organismos del estado en materia de investigación de delitos informáticos, no cuentan con una técnica paso a paso donde el derecho y las técnicas forenses informática vayan de la mano, es por eso que siempre en sus conferencias el Dr. Alexander días García dice que el derecho y las nuevas tecnologías van de la mano en los tipos de investigaciones a través de medios electrónicos donde se debe cumplir con los procedimientos de la ley 527 del manejo de los datos pero utilizando herramientas y programas informáticos en laboratorios especializados donde se cumplan con normas como la iso 27000 / 270001 Seguridad de la información. [36] Todo lo anterior es necesario para poder anclar la información y así nace la cadena de custodia original cumpliendo los procedimientos de la ley sin violar la constitución y se podría anclar la cadena de custodia original sin que en un futuro se vaya a caer la evidencia en un estrado judicial.

## V. CONCLUSIONES

La Constitución Política de Colombia en su artículo 15 permite fundamentar el diseño de la técnica informática en cuanto a la extracción de la evidencia digital para anclar la cadena de custodia, donde se establece el derecho a la intimidad, por lo que se deben respetar la libertad y promover las demás garantías consagradas en la Constitución, apoyado en la Ley 527 de Agosto 18 de 1999 que trata de los instrumentos magnéticos e informáticos, así como la ley 527 de 1999 sobre el comercio electrónico para Colombia, la Ley 1273 de 2009 para la protección de la información y de los datos y la Ley 1273 del 2009 que tipifica los delitos informáticos con el fin de penalizar a los infractores. [32]

A pesar de esto, en Colombia los procesos judiciales en muchos de los casos no ha constituido la evidencia digital como prueba en la resolución de los mismos, ya que los entes encargados como la policía judicial, no han sabido llevar dichas investigaciones judiciales, determinando así el cierre del casos trascendentales por el desconocimiento de un procedimiento que no altere la evidencia digital y la cadena de custodia. [37], [38].

En este sentido, es evidente que se requiere de un procedimiento técnico forense para un sistema de información para que los datos recogidos en la escena criminal estén incólume, a efectos de que el juez autorice la revisión de su contenido y evite que sea alterada la evidencia. [39][40][41].

**REFERENCIAS**


[1] Fiscalía General de la Nación de Santander. Estadísticas de la Unidad de Delitos Informáticos del Cuerpo Técnico de Investigaciones de la Fiscalía General de la Nación de Santander. Bucaramanga: CTI. 2014

[2] Interpol. Informe Forense de INTERPOL sobre los ordenadores y equipos Informáticos de las FARC decomisados por Colombia. 2012. Recuperado de http://www.dragonjar.org/informe-forense-de-interpol-sobre-los-ordenadores-y-equipos-informaticos-de-las-farc-decomisados-por-colombia.xhtml

[3] L. Galván, Propuesta de una metodología de análisis forense para dispositivos de telefonía celular. Esta tesis Doctoral desarrolla una propuesta de metodología forense de telefonía. Instituto Politécnico Nacional. México, México. 2009

[4] H. Rifa, J. Serra, y L. Rivas, Análisis forense de sistemas informáticos. 2009. Recuperado de http://webs.uvigo.es/jlrivas/downloads/publicaciones/Analisis%20forense%20de%20sistemas%20informaticos.pdf

[5] S. Pallela, F. Martins, Metodología de la investigación cuantitativa. Caracas: Fondo Editorial de la Universidad Pedagógica Experimental Libertador. 2006.

[6] F. Arias, El proyecto de Investigación. Bogotá: Editorial Episteme. 2006.

[7] C. Sabino, El proceso de investigación, Lumen-Humanitas, Bs.As., 1996.

[8] C. Ríos, Elementos de lógica epistemología e investigación. (Primera Edición).Bogotá: Editorial Codice ltda. 1996.

[9] Republica de Colombia. Ley 1273 de 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Bogota: Diario Oficial. 2009.

[10] L. Paloma, Delitos informáticos en el ciberespacio. Bogotá: Ediciones Jurídicas. 2012

[11] Departamento Administrativo Nacional de Estadistica Indicadores Básicos de Tecnologías de Información y Comunicación –TIC para Colombia. 2011. Recuperado de http://www.dane.gov.co/files/investigaciones/boletines/tic/bol_tic_2012.pdf

[12] S. Acurio, Delitos informáticos generalidades. 2012. Recuperado de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

[13] A. Díaz, Colombia, el primer país que penaliza los delitos informáticos. 2012. Recuperado de http://www.lapatria.com/tecnologia/colombia-el-primer-pais-que-penaliza-los-delitos-informaticos-1980

[14] L. Cárdena, y M. Becerra, Auditoria forense. 2013. Recuperado de: http://www.gerencie.com/auditoria-forense.html

[15] Policía Nacional. Documentos de la Unidad de Delitos Informáticos. 2014. Cúcuta: DIJIN.

[16] A. Díaz, En busca de cura para los delitos informáticos. 2014. Recuperado de http://www.elespectador.com/noticias/politica/busca-de-cura-los-delitos-informaticos-articulo-492170

[17] Téllez Valdez, Legislación sobre delitos informáticos. 2002. Recuperado de http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml

[18] K. Toaza, Guía Metodológica para el análisis forense en incidentes de teléfono celular con tecnología GSM. Universidad de Guayaqu¿il. Guayaquil, Ecuador. 2011

[19] Fiscalía General de la Nación, Manual de procedimientos del sistema de cadena de custodia. 2004. Recuperado de: file:///C:/Users/USER/Desktop/2004-MANUAL%20CADENA%20DE%20CUSTODIA.pdf

[20] J. Gómez, Hackers aprende a atacar y a defenderse. Bogotá: Alfaomega. 2012

[21] Tribunal Superior de Bogotá, Las irregularidades de la en la cadena de custodia exclusión de la prueba por violación de la legalidad. 2009. Recuperado de http://derechopenalcolombia.blogspot.com/2009_03_01_archive.html

[22] J. León, Los abusos que sufrió Nicolas Castro antes de ser absuelto. 2011. Recuperado de http://lasillavacia.com/historia/los-abusos-que-sufrio-nicolas-castro-antes-de-ser-absuelto-27604

[23] C. Martínez, La informática forense como medio de prueba. 2012. Recuperado de http://www.dragonjar.org/informatica-forense-como-medio-de-pruebas.xhtml

[24] Instituto Español de Estudios Estratégicos. Ciberseguridad retos y amenazas a la seguridad nacional en el ciberespacio. 2013. Recuperado de: http://www.ucm.es/data/cont/docs/71-2013-04-24-71113.pdf

[25] M. López, Análisis Forense digital. 2007. Recuperado de: http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[26] Corte Suprema de Justicia. Sala de casación penal. 2011. Recuperado de http://www.ambitojuridico.com/BancoMedios/Documentos%20PDF/auto%2029877%20(01-08-2011)%20reposici%C3%B3n%20wilson%20borja.pdf

[27] Ministerio de Minas y Energía de Colombia. Sistema de gestión seguridad de la información – SGSI. 2012. Recuperado de: http://www.minminas.gov.co/documents/10180/189141/PoliticaSeguridadInformacion-22Jun2012.pdf/ca680d5d-2dd0-4aff-95d4-21e92687ee0c

[28] Republica de Colombia. Ley 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Bogota: Diario Oficial. 1999.

[29] Malavida. Browser Password Decryptor. 2015. Recuperado de: http://browser-password-decryptor.malavida.com/

[30] Díaz, A. (2014). Apuntes de derecho informático. Bogotá: Habeas Data Consultores.

[31] A. Méndez, Diseño y Desarrollo del Proceso de Investigación. (Cuarta Edición). Bogotá: Limusa Noriega Editores. 2006

[32] Republica de Colombia. Ley 906 de 2004, Por la cual se expide el Código de Procedimiento Penal. (Corregida de conformidad con el Decreto 2770 de 2004). Bogota: Diario Oficial. 2009.

[33] Organización Internacional de Policía Criminal. La Ciberdelincuencia. 2014. Recuperado de http://www.interpol.int/es/Criminalidad/Delincuencia-inform%C3%A1tica/Ciberdelincuencia.

[34] M. López, Análisis Forense Digital. 2007. Recuperado de http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[35] Corte Constitucional. Sentencia C 334/10. 2010Recuperado de http://www.corteconstitucional.gov.co/RELATORIA/2010/C-334-10.html

[36] Boletín Así. Noticias # 23. Análisis Forense. 2004. Recuperado de http://www.auditoria.com.mx/not/boletin/2004/0405_p.html

[37] J. Cano, Computación Forense, Descubriendo Los Rastros Informáticos. Bogotá: Alfaomega. 2013.

[38] Softonic. Cómo ser un detective informático. 2015. Recuperado de: http://articulos.softonic.com/informatica-forense

[39] R. Hernández, L. Fernández, y P. Baptista, Método científico. México: Mcgraw hill . 1998.

[40] J. Cano, Introducción a la informática forense. Revista ACIS. 15(4). 2006. Recuperado de: http://www.acis.org.co/fileadmin/Revista_96/dos.pdf

[41] C. Martínez, Computación forense: descubriendo los rastros informáticos. Editorial Alfaomega. 2009.