Diseño y Plan de Implementación de un Laboratorio De Ciencias Forenses Digitales

Ricardo Gregorio Calderón Valdiviezo [(1)], Gisell Stephanie Guzmán Reyes [(2)], Jessica Margarita Salinas González [(3)], Alfonso Aranda [(4)]
Facultad de Ingeniería en Electricidad y Computación [(1) (2) (3) (4)]
Escuela Superior Politécnica del Litoral (ESPOL) [(1) (2) (3) (4)]
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
rcaldero@espol.edu.ec [(1)], guguzman@espol.edu.ec [(2)], jsalinas@espol.edu.ec [(3)], aaranda@telconet.net [(4)]

Resumen

Se realizó, durante la elaboración del proyecto, un breve análisis de cómo se procedía en el Ecuador ante los delitos informáticos, como se realizaban las investigaciones, y cuál era el trato que se le daba a la evidencia digital. En el trabajo se presentará el plan de implementación de un laboratorio de Ciencias Forenses Digitales donde se podrá aplicar la metodología para la búsqueda y el análisis de evidencias digitales, mediante la aplicación de técnicas científicas y analíticas, conocimientos tecnológicos y legales, para identificar, obtener, reconstruir, analizar y presentar información que pueda ser válida dentro de un proceso legal en donde haya ocurrido un delito informático. La formación de peritos de seguridad informática y el equipo de investigación es parte fundamental en el proceso de rastreo de los orígenes del delito; en este trabajo se buscará definir las funciones y métodos que utilicen los peritos para proceder a la recopilación de datos, pruebas, búsqueda y análisis de evidencias de aplicación en un asunto judicial, ya que para probar un delito deben existir evidencias que relacionen al sospechoso del crimen con el hecho.

Palabras claves: *delito informático, perito informático, laboratorio de ciencias forenses digitales, evidencia digital, análisis.*

Abstract

Was made during the preparation of the project, a brief analysis of how they proceeded in Ecuador to cybercrime as conducting investigations, and what was the deal that gave the digital evidence. The paper will present the plan to implement a digital forensics laboratory where we can apply the methodology to search and analyze digital evidence by applying scientific techniques and analytical, technological and legal expertise to identify, obtain reconstruct, analyze and present information that may be valid within a legal process where a computer crime has occurred. The training of computer security experts and the research team is fundamental in the process of tracing the origins of crime, in this paper seek to define the functions and methods that experts use to carry out data collection, testing, search and analysis of evidence applicable in a court case, and that to prove a crime there must be evidence linking the suspect of the crime with the fact.

Keywords: *computer crime, computer expert, digital forensic science laboratory, digital evidence, analysis.*

1. Introducción

El incremento del uso de medios tecnológicos e información digital ha contribuido para la creación de nuevos nexos de comunicación entre instituciones, empresas y/o personas, de la misma manera ha facilitado el manejo y el almacenamiento de la información, existen personas que utilizan la tecnología para cometer actos ilícitos y causar daños a terceros, convirtiéndose estas conductas en lo que se conoce como delitos informáticos.

Cuando en el cometimiento de un delito se ven involucrados medios tecnológicos e información digital, la forma de llevar a cabo la investigación es diferente a la tradicional; es decir, se deben aplicar metodologías y herramientas especializadas en la recolección y tratamiento de la evidencia digital. Tomando en cuenta estos factores es importante contar con un Laboratorio de Ciencias Forenses Digitales que integre el personal especializado, la infraestructura física y tecnológica, así como también las herramientas de hardware y software adecuadas en el análisis de datos, con el fin de recolectar evidencia que cumpla con los principios de admisibilidad y tenga validez en un proceso judicial. Actualmente, en Ecuador no existe un laboratorio forense digital, por lo tanto, la tarea del esclarecimiento de los hechos involucrados en un delito informático se vuelve más complicada.

2. Evidencia digital

La evidencia digital es catalogada como cualquier información que ha sido generada, almacenada o enviada en un sistema de información y se encuentra comprometida con el delito de manera directa o indirecta [(1)].

2.1. Criterios de admisibilidad

Según el Dr. Santiago Acurio, Director Nacional de Tecnología de la Información, la admisibilidad de la evidencia digital está dada por los siguientes factores [(2)]: establecer un procedimiento de operaciones estándar en el manejo de evidencia, cumplir con los principios básicos reconocidos internacionalmente en el manejo de evidencia digital, cumplir los principios constitucionales y legales establecidos en Ecuador y regirse a la Ley de Comercio Electrónico y el Código de Procedimiento Penal.

3. Peritos informáticos

El análisis forense digital debe ser realizado por el perito informático que es un profesional con conocimiento de fenómenos técnicos en informática, preparado para aplicar procedimientos legales y técnicamente válidos para establecer evidencias en situaciones donde se vulneran o comprometen sistemas [(3)], el mismo debe cubrir las siguientes áreas de conocimiento: Área de tecnologías de información y electrónica, Fundamento de bases de datos área de seguridad de la información, Área jurídica, Área de criminalística y ciencias forenses y Área de informática forense.

El Consejo de la Judicatura establece que para la acreditación de peritos se debe cumplir con los siguientes requisitos [(4)]: ser mayor de edad, poseer una correcta ética profesional, seriedad e imparcialidad en el cumplimiento de tareas asignadas, desvinculación al concluir su trabajo y presentar la documentación requerida: solicitud dirigida al Director Provincial del Consejo de la Judicatura especificando la especialidad pericial, hoja de vida, cédula de identidad y papeleta de votación, en original y copia, record policial actualizado, documentos que acreditan capacitación y experiencias en las materias, comprobante de pago de servicios administrativos. Además, en caso de ser peritos profesionales se requiere que el título haya sido registrado en el CONESUP.

4. Definición de la metodología forense digital

La aplicación de la metodología orientada al análisis de evidencia digital en sus diferentes fases, procura mantener la integridad de la evidencia original, de la misma manera que los resultados presentados al final sean íntegros, confiables y precisos. Para esto se deben cumplir principios o normas de carácter general al realizar el análisis y búsqueda de evidencias digitales, los cuales son: Evitar la contaminación de la evidencia, aplicar metodologías o procedimientos definidos como estándares y controlar la cadena de evidencia [(5)].

4.1. Cadena de custodia

La cadena de custodia es “el procedimiento de control documentado que se aplica a la evidencia física, para garantizar y demostrar la identidad, integridad, preservación, seguridad, almacenamiento, continuidad y registro de la misma” [(6)]. Esta comienza en el lugar donde se encuentra, obtenga o recolecta la evidencia física y solo finaliza cuando la autoridad competente lo ordene, durante este proceso se siguen varias etapas que presentamos a continuación: [(7)] [(8)]

4.1.1. Recolección, clasificación y embalaje de la prueba. La cadena de custodia empieza en la escena del delito por lo cual es fundamental el aseguramiento de la misma con el fin de evitar la contaminación de la evidencia, es necesario seguir los siguientes pasos:

Aislar, identificar y registrar en un acta los equipos informáticos y las personas que trabajen en estos. **Registrar y fotografiar** todos los elementos antes de moverlos o desconectarlos. **Documentar la hora y la fecha del sistema** si se encontraran equipos encendidos antes de proceder a apagarlos. Y si se encontraran apagados se procede únicamente a desconectarlos desde la toma del equipo. **Identificar y clasificar** la evidencia encontrada de acuerdo a su naturaleza, y llenar el acta respectiva.

4.1.2. Embalaje de la evidencia. Se debe de registrar el nombre del oficial encargado del embalaje, etiquetado y clasificación de la evidencia encontrada ya que él será el encargado de su traslado hasta los almacenes de custodia. En esta etapa se recomienda etiquetado y rotulación que permitan una fácil ubicación e identificación de la evidencia.

4.1.3. Custodia y traslado de la evidencia. El oficial que realizó el embalaje, clasificación y etiquetado de la evidencia será el encargado de trasladarla al almacén del laboratorio, y este permanecerá en el lugar hasta que la evidencia sea aceptada e ingresada por la persona encargada de la custodia de la misma. En caso contrario, se documentará el cambio de custodia.

Una vez ingresada al Laboratorio de Ciencias Forenses Digitales, se procede a realizar el registro de entrada de la evidencia digital completando el formulario Ingreso de Evidencia. Posteriormente se procederá a almacenar la evidencia en recipientes especiales, con aislamiento y será almacenada en una habitación con seguridades físicas, a la cual solo podrá acceder personal del laboratorio que cuente con la debida autorización. Todo traslado de la evidencia dentro y fuera del laboratorio será registrado llenando el formulario de Entrada y Salida de Evidencia del laboratorio.

4.1.4. Análisis de la evidencia. Para realizar el o los análisis el perito encargado debe de solicitar al almacén del laboratorio la prueba a la cual le va a efectuar los análisis, procediendo al llenado de las actas respectivas de entrega de evidencia que se encuentran en el almacén. Previamente se debe de revisar el recipiente que contiene la evidencia y registrará las condiciones en que se encuentra en el formato que maneja el laboratorio. Así mismo el perito encargado del análisis de la evidencia digital tiene la obligación de obtener el número de copias idénticas de la muestra, necesarias para realizar los análisis respectivos y de llevar una bitácora de análisis, en la cual se registrará cada uno de los procedimientos que se realizan sobre la evidencia, así como la justificación del análisis, las observaciones o inconvenientes que se presenten durante el análisis.

Posterior a la finalización del análisis, toda evidencia debe ser devuelta al almacén del laboratorio para su almacenaje, el encargado del almacén debe de registrar el ingreso de la evidencia y debe de etiquetarlas con una codificación para que sea posible su ubicación para nuevos análisis o para su destrucción.

4.1.5. Custodia y preservación final hasta que se realice el debate. La evidencia tendrá que ser recibida por el personal encargado del almacén del laboratorio, el cual debe de registrar la fecha y hora de recepción del material así como el nombre del perito que hace entrega de la misma y verificar el estado en que fue recibida y almacenarla siguiendo códigos que faciliten la localización para futuros análisis y/o destrucción según sea el caso.

4.2. Procedimientos técnicos

Los procedimientos técnicos aplicados a las evidencias digitales deben ser implementados guardando la integridad y confiabilidad de las evidencias digitales.

4.2.1. Recolección de evidencia digital. Se deben tomar decisiones y precauciones para mantener la evidencia intacta y libre de contaminación externa, una de las primeras decisiones que se debe tomar es con respecto a un computador encontrado en la escena de los hechos, ya que se debe de tomar en cuenta que si es apagado inmediatamente puede existir pérdida de memoria RAM y si no se apaga existiría la posibilidad de que se ejecute una bomba lógica.

Para apagar el computador, que es evidencia se recomienda seguir las siguientes indicaciones: No apagar el equipo desde el botón que cumple esta función, Si el computador no se encuentra bloqueado, se debe poner el computador en modo suspensión y proceder a desconectar el cable de alimentación eléctrica desde la fuente del poder del computador, de esta manera los datos pasan al disco duro.

Al finalizar el allanamiento, para el traslado de las pruebas se procede como se indica en la sección 4.1.1 de la cadena de custodia.

Realizar copias de la prueba original. De los elementos donde se espera encontrar pruebas, se debe realizar por lo menos una copia del original sobre la que se realizaran todos los análisis.

Para realizar la copia del contenido original del computador, se debe extraer el disco duro siempre tomando las medidas de seguridad adecuadas para proteger la evidencia. Si no es posible extraer el disco duro, se debe modificar la secuencia de arranque en el BIOS del sistema y arrancar con un sistema operativo desde un CD, sin instalar nada en el sistema. También se puede realizar la copia de las evidencias digitales como información en archivos de texto, imágenes, entre otros que están almacenadas en discos duros mediante utilización de software especializado que no altere la evidencia y esta pueda ser aceptada en un proceso judicial [9] [10].

Retención de tiempos y fechas [10]. Durante el análisis, siempre que sea posible se debe trabajar con zonas de tiempo GMT o cualquier otro estandarizado. **Generar los procesos de suma de verificación criptográfico de la evidencia digital (copia y original) [10].** Se genera un proceso de suma de verificación de la evidencia original y de las copias para garantizar que esta no ha sido alterada durante el análisis, para esto usamos el algoritmo de suma de verificación MD5.

4.2.2. Identificación de las evidencias digitales. Debido a que en los sistemas de información es posible encontrar evidencia digital heterogénea, lo mejor es realizar una clasificación de las evidencias digitales en evidencias digitales en medios volátiles y en medios no volátiles. Las evidencias digitales en medios volátiles desaparecen ante la falla de alimentación eléctrica o falla de conexión, se puede encontrar en la memoria RAM, cache. Mientras que las evidencias no volátiles perduran aún con la interrupción de alimentación eléctrica, se pueden encontrar en unidades de disco duro.

4.2.3. Análisis de las evidencias digitales. La evidencia digital normalmente se forma por el contenido de los ficheros o datos y la información sobre los ficheros (metadatos). Basándose en estas evidencias el investigador debe tratar de contestar las preguntas de: [10].

¿Qué?: Determinar la naturaleza de los eventos ocurridos.

¿Cuándo?: Reconstruir la secuencia temporal de los hechos.

¿Cómo?: Descubrir que herramientas o piezas de software se han usado para cometer el delito.

¿Quién?: Reunir información sobre los involucrados en el hecho.

Durante el análisis se extrae información relevante del caso para recrear la cadena de eventos sucedidos, por lo tanto se requiere noción de lo que se está buscando y como obtenerlo. Para lograr este cometido nos ayudaremos de herramientas de hardware y software especializado, tales como el encase, deft-extra, forensic tool kit, entre otras, las cuales nos ayudara a recolectar información relevante del sistema y comunicaciones que se han tenido por medio del equipo.

4.2.4. Análisis de dispositivos móviles. El dispositivo debe ser totalmente cargado previo al examen, se debe considerar tener una fuente de alimentación de energía fija o portátil. El análisis se debe empezar con una copia de la información que se extrae del dispositivo, para el análisis de de dispositivos móviles haremos uso de software especializado como el Oxygen Forensic Suite. El cual nos permite obtener toda la información que se encuentre almacenada en los diferentes tipos de memorias de un dispositivo móvil, tal como [11]: Tarjeta SIM, memoria externa y memoria interna.

4.2.5. Presentación de resultados. La elaboración del reporte de los resultados detalla las evidencias encontradas durante el análisis, presenta cada procedimiento realizado a cada una de ellas, justificándolos para darle validez a la evidencia digital, replantea los hechos y determina las conclusiones. Este reporte debe de presentar la información relevante de manera clara, concisa, estructurada y sin ambigüedad, evitando la terminología técnica. Con la finalidad de ser usados frente a la corte con el objetivo de probar el delito que se ha llevado a cabo.

5. Diseño del laboratorio de Ciencias Forenses Digitales

Analizaremos las condiciones físicas, ambientales e infraestructura para la adecuación del Laboratorio, de la misma manera el hardware y software necesarios para el análisis forense digital.

5.1. Instalaciones

Las instalaciones deben de garantizar la integridad y la seguridad de la evidencia, es por

esto que contará con medidas de seguridad que permitan el acceso solo a personal autorizado.

5.1.1. Seguridades físicas. Acceso mediante sistema biométrico, y cerradura, previo a la identificación de la persona que desea ingresar. También, contará con un sistema de video de circuito cerrado en todas las áreas, que grabará los acontecimientos dentro del laboratorio durante las 24 horas, y se instalará un sistema de alarma con sensor de movimientos que se encontrará intercomunicado con la estación de policía más cercana y con un equipo de guardianía privada.

Todo el personal que labore dentro de las instalaciones deberá de portar la credencial otorgada por el laboratorio en todo momento y en un lugar visible. Por lo general no se aceptan visitas al laboratorio, pero en el caso de existir, esta deberá presentar una identificación y será anunciado con la persona con quien desea comunicarse para luego ser atendido en el área anexa de Control de Acceso y Entrada.

5.1.2. Condiciones ambientales. El laboratorio debe poseer las condiciones ambientales ideales para no invalidar el resultado de los análisis ni la calidad requerida, así mismo el estado de las evidencias digitales originales [12] [13] [14].

Con respecto a la esterilidad biológica se recomienda desinfectar la superficie de trabajo con lejía al 2%. Los dispositivos electrónicos deben estar protegidos de la interferencia electromagnética, para lo cual se recomienda el uso de jaulas de Faraday, y para evitar saltos de voltaje se recomienda el uso de UPS y un generador eléctrico. El ruido y la vibración son contaminantes que pueden evitarse utilizando materiales aislantes en la construcción del laboratorio.

El sistema de climatización e instalación de filtros evita el paso de polvo, la humedad, el sobrecalentamiento y deterioro de los equipos de cómputo, es recomendable manejar un correcto sistema de refrigeración con una temperatura estable de 22°C y mantener un límite de humedad máximo del 65% dentro de las instalaciones.

Sistema de extinción de incendios que este adecuado al material eléctrico y magnético, que se va a manejar dentro de las instalaciones, para tratar de causar el menor impacto en caso de su uso, tales como polvo químico seco o bióxido de carbono , espuma, INERGEN, entre otras.

5.1.3. Despliegue de infraestructura en el interior del laboratorio. Las instalaciones deberán contar con elementos esenciales, tales como [15] [16]: Cableado de red con puntos de red en todas las áreas del laboratorio, cableado telefónico, UPS o generador eléctrico en caso de falta de energía eléctrica. Con respecto al lugar las habitaciones deben ser en lo posible sin ventanas a la parte externa del laboratorio y con divisiones con paneles móviles para las distintas áreas.

En el diseño que planteamos las instalaciones estarán divididas en tres áreas: almacenamiento, mecánica y análisis. El área de almacenamiento [17] contará con un cubículo previo con una puerta de acceso, con seguridad multilock, a la ubicación de los armarios de evidencia, contará con un Área de Control de Acceso y Entrada, que será el lugar donde se atenderá a las personas que soliciten alguna prueba para su análisis, ningún personal sin autorización podrá acceder más allá del Área de Control de Acceso y Entrada. Los armarios de almacenamiento de evidencia que llega al laboratorio para el proceso de investigación y para su almacenaje posterior tendrán acceso restringido y se registrará la hora y el nombre de quien acceda a ella.

Se tomarán precauciones para el correcto almacenamiento de la evidencia dependiendo de la naturaleza de la misma, usando contenedores antiestáticos y/o esponja antiestática, lo que ayudará a aislar de fuentes eléctricas y de campos magnéticos, que puedan corromper la información contenida en los dispositivos digitales durante su almacenamiento y transporte.

En el área mecánica, se realizará el desmontaje, ensamblaje y manipulación física de un computador, en caso de que se necesite analizar un computador completo, esto es para que sus partes puedan ser analizadas por separado si las circunstancias lo ameritan [16]. Para llevar a cabo la tarea de desmontaje, se dispondrán de herramientas necesarias, así como de equipos especializados.

El área de análisis tendrá tres puestos de trabajo cada uno con un armario respectivo. Todas las áreas serán de libre acceso, solo se contará con una puerta de entrada principal a las instalaciones del laboratorio.

Para llevar a cabo todas las tareas que están incluidas en el análisis de la evidencia, esta área contará con las herramientas de análisis forenses que se dispongan tanto hardware como software. Existirán dos zonas, una de la cuales tendrá acceso a internet en la cual se podrán realizar investigaciones, que se necesiten dentro del proceso de análisis, y la otra zona no tendrá

acceso a internet para evitar cualquier intervención externa en el análisis de la evidencia.

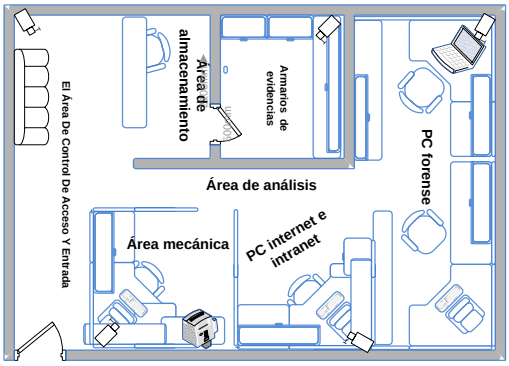

Figura 1. Diseño del laboratorio

5.2. Equipos informáticos

El conjunto de equipos de trabajo en el laboratorio de Ciencia Forense Digital, integra herramientas especializadas, computadores de escritorio y portátiles para llevar a cabo el proceso de análisis forense.

Herramientas de duplicación de discos con alta velocidad de copiado, conectividad con las diferentes interfaces de discos duros, adaptadores, portabilidad, esto permitirá realizar copias de discos duros los cuales se usarán para los análisis de las pruebas de una manera fácil y rápida. Además se contará con dos tipos de equipo en las instalaciones el equipo base que será una desktop y un equipo portátil que será una laptop con similares características que el equipo base.

5.3. Software utilizado

Existen varios tipos de herramientas entre las cuales hemos escogido dos, que son Deft-Exra (software libre) y Encase (software privado) las cuales cumplen con características importantes como: Clonación de discos, comprobar integridad criptográfica, dar información del sistema, adquisición en vivo, recuperación de contraseñas, análisis forense en redes, análisis forense en navegadores, búsqueda de archivos, utilitarios extras, entre otros. Se puede hacer uso de software complementario si fuese necesario para las tareas que no puedan desempeñar estas dos herramientas.

5.4. Posibles ubicaciones en la ESPOL

Dentro de las instalaciones de la ESPOL se encuentran tres áreas disponibles que podrían ser utilizadas para la implementación del laboratorio, las cuales son: el aula de capacitación ubicada en el edificio del CSI, la sala de ayudantes ubicada en el segundo piso del edificio 15A de la FIEC, y la oficina del VLIR ubicada en el edificio 16C de la FIEC.

La alternativa ideal que hemos escogido se encuentra en las instalaciones del CSI, aula, que actualmente es utilizada como sala de capacitaciones, está ubicada frente a la entrada principal y junto a la sala de servidores del CSI.

Dentro de las ventajas de esta opción esta el acondicionamiento, esta aula cuenta con un sistema de aire acondicionado ideal para el desempeño de las actividades a desarrollarse, además cuenta con sistema de alarma con sensores de movimiento y sistema contra incendio automático, lo cual supondría un ahorro en la inversión inicial del laboratorio. También cuenta con una habitación que se la puede acondicionar como el almacén de evidencia, su tamaño mediano (aproximadamente 40mts2).

Como desventajas esta la ubicación ya que hace que sea un poco complicado de llegar, para personas que no conocen la ESPOL, Cuenta con una pared completamente de vidrio que une a la sala de servidores del CSI lo cual supondría una inversión en su cambio por una pared de cemento, habría que realizar una impermeabilización de su techo ya que hay alguna filtración en época de lluvia.

6. Resultados

De acuerdo a las condiciones y los elementos ideales planteados en este trabajo para la implementación de un laboratorio de ciencias forenses digitales en la ESPOL determinamos los costos de la integración de todos los elementos necesarios en este laboratorio, el cual estaría ubicado en las instalaciones del CSI, tendría un diseño en el que se incluyen divisiones con paneles móviles y más seguridad en el área de almacenamiento. Para el análisis proponemos utilizar hardware forense especializado y software comercial por su estabilidad y soporte.

Tabla 1. Detalle de precios

	Alternativa Uno
Inversión Inicial	11.291,40
Hardware y Software	43.027,74
Total	**54.319,14**

La inversión inicial incluye el valor del sistema de seguridad, las adecuaciones al lugar y los demás implementos de seguridad contra incendios.

7. Conclusiones

Para la implementación del laboratorio de Ciencia Forense Digital se necesita una inversión de la cual el mayor porcentaje sería destinado a la adquisición de hardware y software, el porcentaje restante se utilizará en seguridad y adecuación del laboratorio como sistemas de alarma, sistema de climatización, entre otros.

Todo el personal que está involucrado en la investigación de un delito, el personal de la policía que realiza el allanamiento en el lugar de los hechos, y los agentes fiscales, no cuentan con la capacitación adecuada para el tratamiento de evidencia digital, esto tiene como consecuencia el retraso de la investigación, la alteración de la evidencia y de los resultados que se podrían obtener.

Se recomienda el uso de firmas digitales para la emisión de órdenes judiciales, esto sería de gran utilidad para agilizar el proceso de obtención de evidencia en la escena del crimen y en el caso de los ISP podrían entregar información con la certeza de que la orden judicial es original. El proceso se llevaría a cabo de la siguiente manera: el Juez de Garantía Penales emitiría la orden con su firma digital y la enviará por correo electrónico y ésta podrá ser recibida y verificada por el Fiscal que solicitó la orden quedando así aprobado el allanamiento y el secuestro de evidencia.

8. Recomendaciones

Implementar un Laboratorio en la ESPOL que plantee un referente en investigación Forense Digital, y que preste sus servicios a entidades públicas y privadas.

Capacitar a los miembros involucrados en el control de la cadena de custodia, en el tratamiento de evidencia para que tenga validez en un proceso penal ante un juez.

9. Referencias

[1] Ghosh Ajoy, HB:171:2003 Guidelines for the Management of IT Evidence - 2003. United Nations Public Administration Network,http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf, Fecha de consulta 10 de Abril 2011.

[2] Acurio Santiago, Perfil sobre los delitos informáticos en el Ecuador - Alfa-Redi: Políticas de la Sociedad de la Información, http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/acurio1.pdf, fecha de consulta 10 de Abril del 2011.

[3] Cano Jeimy, Estado del Arte del Peritaje Informático en Latinoamérica. Alfa-redi: Políticas de la Sociedad de la Información, http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/374d0ee90831e4ebaa1def162fa50747/Estado_del_Arte_del_Peritaje_Informatico_en_Latinoamerica.pdf, fecha de consulta 10 de Abril 2011.

[4] Función Judicial, Consejo judicatura, Normativa Que Rige Las Actuaciones Y Tabla De Honorarios De Los Peritos En Lo Civil, Penal Y Afines, Dentro De La Función Judicial, http://www.funcionjudicial.gov.ec/www/pdf/resoluciones/resolucion%2031%20de%20julio%20de%202009.pdf, fecha de consulta 10 de Abril 2011.

[5] S.G.K. Publiguía de Internet, Principios Forenses, http://www.segurinfo.es/?Contenido=Contenido.asp&CAId=501, fecha de consulta 1 de Mayo 2011.

[6] Slideshare, Cadena de custodia, http://www.slideshare.net/luchotoribio/cadena-de-custodia-colombia, fecha de consulta 1 de Mayo 2011.

[7] Gómez Leopoldo Sebastián - Revista Informática Alfa-Redi, Guía Operativa para Procedimientos Judiciales con secuestro de tecnología Informática, http://www.alfa-redi.org/rdi-articulo.shtml?x=6216, fecha de creación 5 de Junio 2006.

[8] Fiscalía general de la nación Colombia, Manual del sistema de cadena de custodia, http://www.usa.edu.co/derecho_penal/2004-MANUAL%20CADENA%20DE%20CUSTODIA.pdf, fecha de consulta 1 de Mayo 2011.

[9] Microsoft, Guía fundamental de investigación informática para Windows, http://technet.microsoft.com/es-es/library/cc162837.aspx, fecha de creación 11 de Enero 2007.

[10] Code of practices for digital forensics, Código de Prácticas para Digital Forensics, http://cp4df.sourceforge.net/flashmob03/doc/03-Metodologia-rev3.pdf, fecha de consulta 1 de Mayo 2011.

[11] Revista Digital Universitaria, Dispositivos móviles, análisis forenses, http://www.revista.unam.mx/vol.9/num4/art26/int26.htm, fecha de creación 10 de Abril 2008.

[12] Scribd, Instalación de Centros de Cómputo, http://es.scribd.com/doc/4555611/Instalacion-de-Centros-de-Computo, fecha de consulta 26 de Abril 2011.

[13] Seguridad en América, Protección contra incendios en sites de cómputo, http://seguridadenamerica.com.mx/2010/04/proteccion-contra-incendios-en-sites-de-computo/, fecha de creación 8 de Abril 2010.
[14] Jorge Antonio, Medidas De Prevención De Un Centro De Computo, http://jorgeantonio.soy.es/, fecha de creación 26 de Octubre 2009.
[15] Gómez Leopoldo - Pericias informáticas, Guía de implementación de un laboratorio de informática forense, http://periciasinformaticas.sytes.net, fecha de creación 1 de Enero 2009.
[16] UNIVO, Diseño de centro de cómputo, http://www.univo.edu.sv:8081/tesis/014213/014213_Cap5.pdf, fecha de consulta 15
[17] NCJRS, Forensic Laboratories: Handbook for Facility Planning, Design. Construction, and Moving, http://www.ncjrs.gov/pdffiles/168106.pdf, fecha de consulta 26 de Abril 2011.